ELABORACIÓN DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN

Nombre Estudiante: Ruth Aguilar Escobar

Programa: Proyecto Final de Posgrado en Gestión y Auditoria de la Seguridad

Nombre Consultor: *Arsenio Tortajada Gallego*

Centro: Universitat Oberta de Catalunya

Data Entrega: Junio 2017


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SenseObraDerivada 3.0 España de Creative Common

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un plan de seguridad de la Información*
Nombre del autor:	*Ruth Aguilar Escobar*
Nombre del consultor:	*Arsenio Tortajada Gallego*
Fecha de presentación:	*06/2017*
Área del Trabajo Final:	*Gestión y Auditoria de la Seguridad*
Titulación:	Proyecto Final de Posgrado en Gestión y Auditoria de la Seguridad

Resumen del Trabajo (máximo 250 palabras):

El presente proyecto ha consistido en la elaboración de un Plan de Seguridad de la Información para la empresa A2, un proveedor de servicios financieros. Este plan de seguridad se basa en el estándar internacional ISO/IEC 27001 y la guía de buenas prácticas ISO 27002:2013.

El proyecto comporta de 5 fases:

En la fase 1 se ha descrito la organización sobre la que se implanta el proyecto y se ha realizado un análisis diferencial de la situación actual de la seguridad con respecto a las normas.

En la fase 2 se han definido los documentos de base necesarios para el cumplimiento normativo: política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por la Dirección, gestión de roles y responsabilidades, declaración de aplicabilidad y la metodología de análisis de riesgos.

En la fase 3 se ha realizado el análisis de riesgos siguiendo la metodología MAGERIT v3.

En la cuarta fase se han planteado 11 proyectos para mitigar los principales riesgos y mejorar la seguridad de la información.

En la fase 5, se ha realizado una auditoria de cumplimiento para medir el cumplimiento de los diferentes dominios con respecto a la norma. Se han identificado no conformidades y se han propuesto acciones correctoras .

En base a los resultados obtenidos se concluye que la implantación del plan director de seguridad ha mejorado el nivel de seguridad de la información en la empresa.

Palabras clave (entre 4 y 8):

Activo, Riesgo, Seguridad, Cumplimiento, Amenaza, Vulnerabilidad

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

En toda empresa independientemente del tamaño y del sector en la que desenvuelve, los activos mas importantes a proteger son la información y los sistemas de información. Es importante para las empresas garantizar un manejo seguro de la información (numérico o físico).

Es a través del conocimiento del estado actual del manejo de la información que se pueden identificar las deficiencias en materia de seguridad y así proponer mejoras buscando garantizar un manejo seguro de la información.

El establecimiento de un plan de seguridad de información mejora la competitividad de la empresa, conduce a un mayor crecimiento y a la obtención de mayores beneficios. Preserva y mejora la reputación de la empresa, conduce a cumplir con los requisitos legales, y sobre todo genera confianza a los clientes, socios y otras organizaciones con las que la empresa interactúa.

1.2 Objetivos del Trabajo

Elaborar un plan director de seguridad de la Información de la Empresa A2 que sea una guía corporativa para la implantación de las medidas de seguridad de la información y los sistemas de información dentro de la organización.

1.3 Enfoque y método seguido

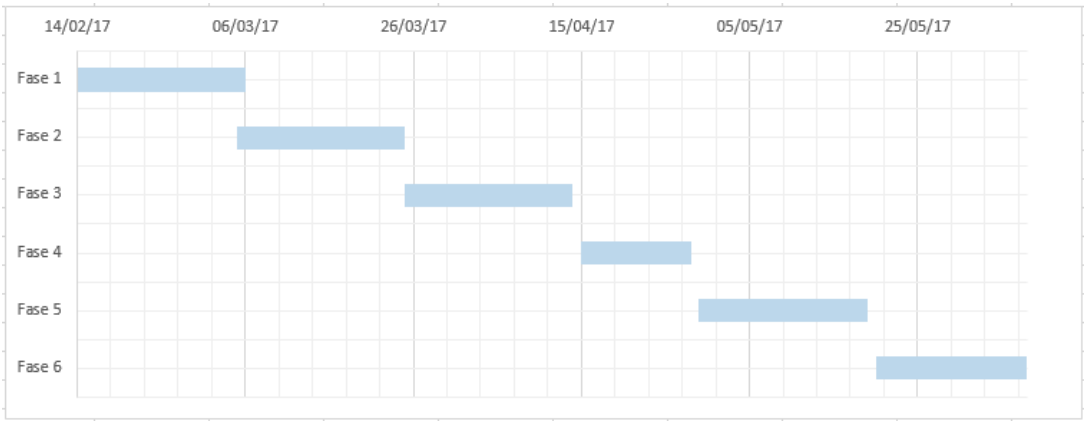
El plan se basa en la norma ISO27001 y la ISO27002:2013, y por consiguiente en el ciclo de Demming (PDCA), basado en la planificación de actividades, su implementación y operación, su revisión y su posterior mejora.

El enfoque que se sigue para este plan ha sido estructurada en cinco fases que son: Situación actual , Sistema de Gestión Documental, Análisis de riesgos, propuesta de proyectos y Auditoria de cumplimiento

Es a través de la implementación del plan que se pretende garantizar la actualización del Sistema de Gestión de la Seguridad de la Información y por consiguiente la mejora continua en el manejo de la seguridad.

1.4 Planificación del Trabajo

Fases		Inicio	Días	Fin
Fase 1	Situación Actual: Contextualización, objetivos y análisis diferencial	14/2/17	20	4/3/17
Fase 2	Sistema de Gestión Documental	5/3/17	20	24/3/17
Fase 3	Análisis de Riesgos	25/3/17	20	14/4/17
Fase 4	Propuestas de Proyectos	15/4/17	13	28/4/17
Fase 5	Auditoria de cumplimiento de ISO/IEC 27002:20013	29/4/17	20	19/5/17
Fase 6	Presentación de Resultados y entrega de Informes	20/5/17	18	7/6/17



1.5 Breve sumario de productos obtenidos

Los entregables resultado de este proyecto son:

- Informe de análisis diferencial: que permite conocer el estado actual de la organización en relación a la seguridad de la información.
- Esquema documental básico establecido por la norma, que establece las bases del SGSI, y sobre los cuales se lleva a cabo las diferentes actividades del proyecto.
- Análisis de Riesgos que comprende: un análisis detallado de los activos relevantes a nivel de seguridad de la empresa, un estudio de la posibles amenazas sobre los sistemas de información y de su posible impacto en las mismas. Una evaluación del impacto potencial que tendría la materialización de las diferentes amenazas a los que están expuestos los activos.
- Propuesta de proyectos que resultan de recomendaciones identificadas durante el análisis de riesgos y que con su implantación en la organización ayudaran a mitigar los riesgos y permitir una evolución hasta un nivel adecuado de la norma.
- Informe de auditoria de cumplimiento: que refleja el nivel de cumplimiento/incumplimiento de la seguridad de la empresa con relación a los diferentes dominios del ISO/IEC 27002:2013.

- Informes globales: Un Resumen ejecutivo, una memoria de proyecto, defensa en formato PPT y un video de la defensa.

1.6 Breve descripción de los otros capítulos de la memoria

La memoria consta de 6 capítulos y cuyos objetivos se describen a continuación:

- Capitulo 1: Justificar, definir el objetivo, describir el enfoque, planificar el trabajo y describir los entregables resultados de este trabajo.
- Capitulo 2: Describir y conocer la organización en la que se implementara el proyecto de seguridad de la información y la situación actual en materia de seguridad frente a la norma ISO/IEC 27002:2013.
- Capitulo 3: Definir las bases documentales, normativas y metodológicas sobre las cuales se implementará el SGSI en la entidad soportados en la propia norma ISO/IEC 27001.
- Capitulo 4: Identificar y evaluar los activos más importantes de la entidad, así como los riesgos inherentes a los mismos definiendo la probabilidad y el impacto de la materialización de los mismos.
- Capitulo 5: Proponer proyectos que a través de su implementación buscan mitigar los riesgos de seguridad de la información.
- Capitulo 6: Medir el nivel de cumplimiento de la seguridad de la empresa frente a la norma ISO/IEC 27001:2013, concretamente en lo que respecta los 114 controles del anexo A.

2 Fase 1: Situación Actual

2. 1 Contextualización

La empresa A2 es una empresa líder en la provisión de soluciones financieras y de pensiones. Actualmente es líder entre las empresas de seguros con un importante numero de clientes particulares y empresariales.

Es una empresa experta en la protección y en los seguros de vida, ofrece soluciones, tanto en la protección de los ingresos de los particulares como en la protección de las empresas, la planificación de pensiones, planificación patrimonial y la acumulación de riqueza. La empresa A2 también brinda consejería a los empresarios que quieran establecer una política de "beneficios de los empleados" equilibrada.

Siendo la empresa A2 un proveedor de servicios financieros, es de mucha importancia asegurar un manejo seguro de la información y de sus sistemas de información.

Para la empresa el éxito comercial esta relacionado con la integridad, la confidencialidad, el buen emprendimiento, la solidez financiera, un enfoque de los objetivos a largo plazo y la gestión avanzada de los riesgos. La empresa A2 busca ser transparente y ética en todas las actividades que realiza, tomando en cuenta todas las dimensiones del desarrollo sostenible buscando equilibrar los intereses de todos los grupos de interés.

Características principales

1. Forma parte de un grupo internacional con sedes en diferentes países
2. La plantilla para el país cuenta actualmente de 250 empleados sin contar con los consultores externes y/o corredores independientes.
3. El 60% de la cartera corresponde a los seguros de vida
4. La empresa cuenta con dos sedes, una central donde se encuentran las oficinas para todos los departamentos, incluyendo las oficinas IT. Una segunda sede que se ubica a 100km de la sede central y en la que se encuentra la infraestructura tecnológica y de almacenamiento masivo de la información digital. Solo un grupo reducido de personal tiene sede el segundo centro.
5. Todos los empleados de la empresa pueden trabajar 2 días a la semana desde sus hogares. Siendo también posible trabajar a distancia mas días por semana.
6. La empresa cuenta actualmente con un gran numero de consultores externos en los diferentes departamento, pudiendo estos trabajar en la sede central o remotamente desde otros lugares.
7. El acceso a las redes de la empresa y la información se realiza solo por medio de los equipos (pc's, portables, tabletas, celulares, etc.) que la empresa pone a disposición del personal.

8. La sede central ocupa un edifico de 6 pisos, en lo que se encuentran todos los departamentos, directivos y personal, las salas de reuniones, conferencias, cafetería, etc.
9. La segunda sede ocupa un establecimiento de dos plantes. Esta sede alberga todo la infraestructura tecnológica y el personal que garantiza su funcionamiento. Esta sede no esta disponible para el resto del personal ni el personal externo.

Organigrama de la empresa

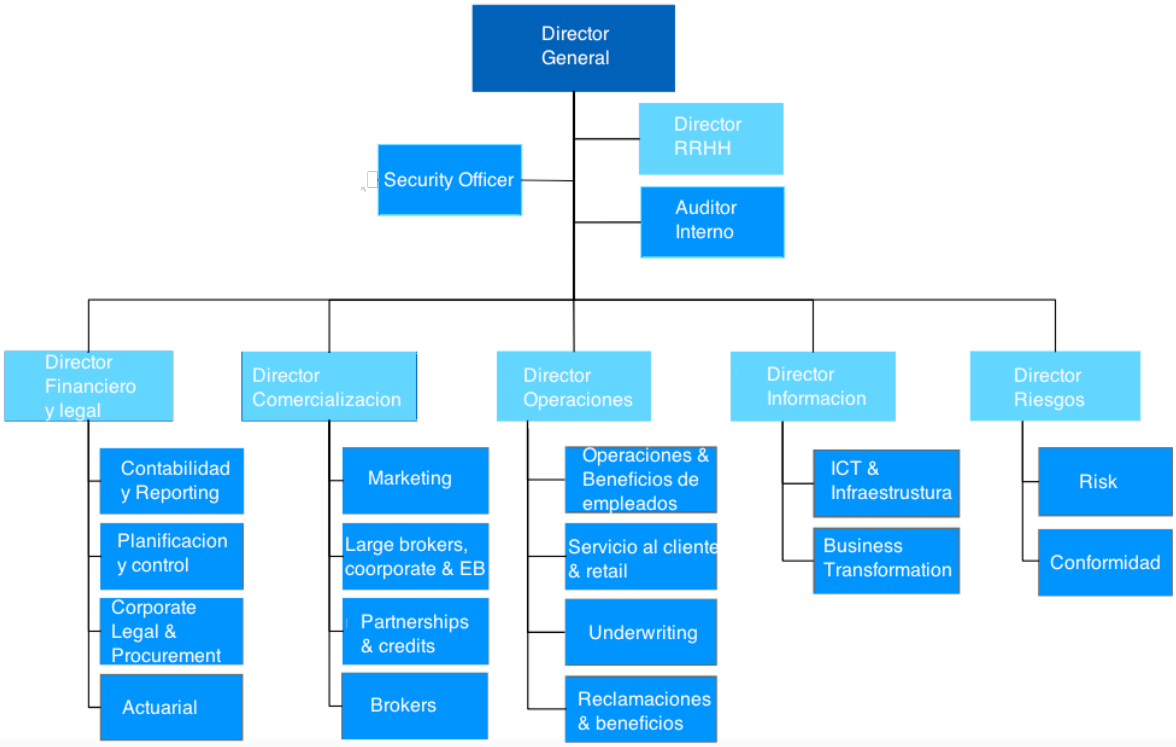


Fig. 1: Organigrama de la empresa A2

Repartición del personal interno de la empresa

Departamento	No de personas
Dirección General	5
RRHH	10
Finanzas y legal	5
Contabilidad y reporting	11
Planificación y control	5
Corporate Legal & procurement	4
Actuarial	4
Comercialización	2
Marketing	20
Large Brokers, coorporate & EB	5
PartnerShips & credits	10

Brokers	13
Operaciones	13
Operaciones & Beneficios de empleados	20
Servicio al cliente & retail	30
Underwriting	12
Reclamaciones & Beneficios	20
Información	2
ICT & Infraestructura	55
Business transformation	15
Riesgos	3
Riesgo	6
Conformidad	4

Diagrama simplificado de la red de la empresa

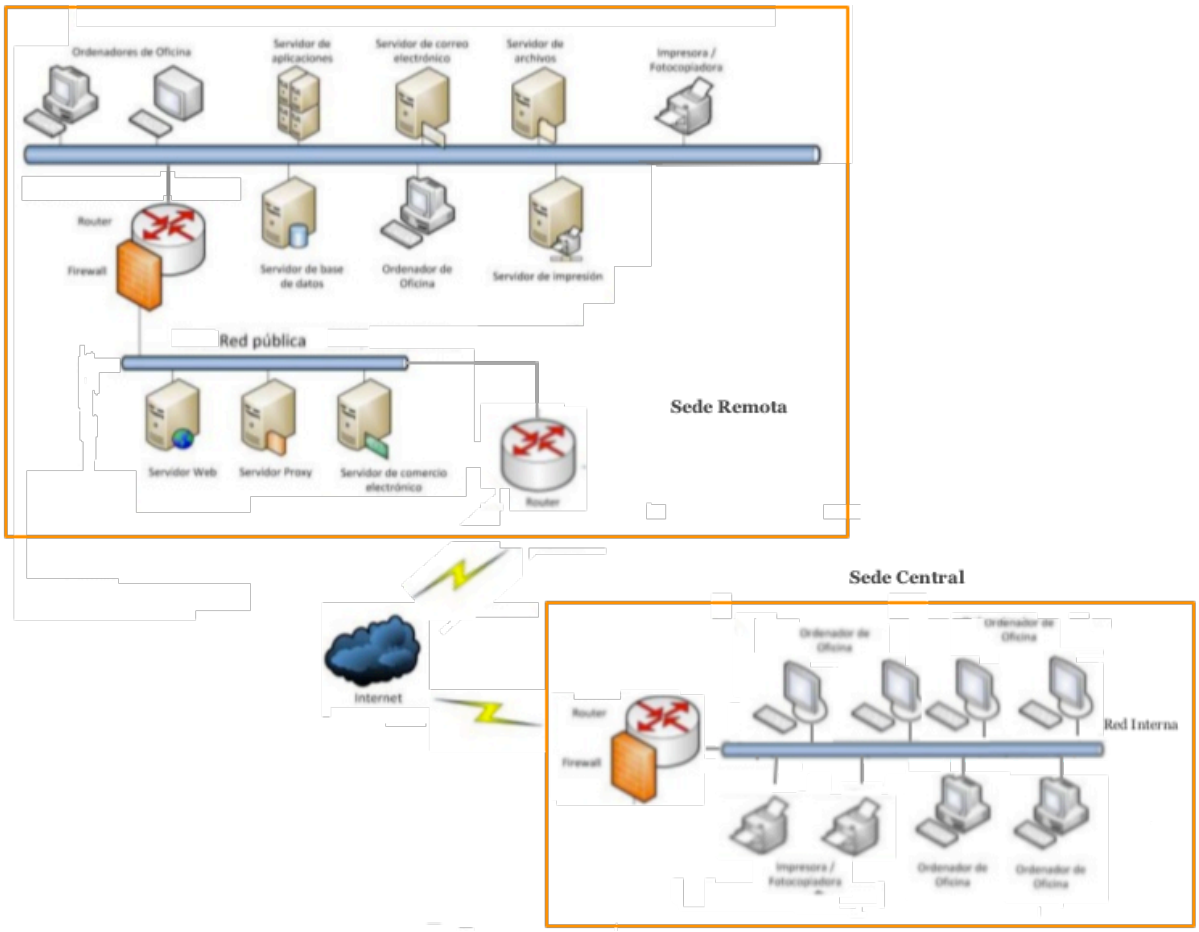


Fig. 2: Diagrama simplificado de red

Principales equipos de procesamiento y manejo de la información

- Pc portables para cada empleado (Windows 7)
- Los servidores Unix

- Los servidores de bases de datos – Oracle
- Servidores Windows
- Los servidores mail
- Los proxis server
- Servidores de aplicaciones
- Content Servers
- File Servers
- Backup Servers
- Impresoras
- Fotocopiadoras/scanners
- Teléfonos
- Celulares
- Tabletas

Aplicaciones de software

La empresa cuenta con sus propias aplicaciones para el procesamiento de los datos de los clientes (particulares y/o empresariales). Existen aplicaciones para los diferentes productos y servicios que oferta. Aplicaciones para el manejo de cuentas particulares, aplicaciones para el manejo de cuentas empresariales.

El acceso a las aplicaciones por parte del personal es a través del portal interno de la empresa. El acceso a este portal es a través de una clave única asignada a cada empleado en el momento de la contratación. El alcance de sus accesos es en función al rol y las responsabilidades que tengan al interior de la empresa.

Los clientes particulares o empresariales tienen acceso a los diferentes servicios por medio de un portal externo que requiere la autenticación con la carta id. Es a partir de esta entrada que pueden acceder a su diferentes espacios para consultar sus datos y realizar sus transacciones.

Los sistemas de información que dispone la empresa se resumen en las siguientes categorías:

- Aplicaciones de contabilidad propias de la empresa.
- Aplicaciones para la gestión de recursos humanos
- Aplicaciones para el manejo de productos y servicios (vida, deceso, rama21, rama23, seguro de grupo, saldo restante, etc.)

Seguridad Física

1. Casa empleado posee una tarjeta de acceso a la empresa y a departamentos predeterminados.
2. Cada empleado se le asigna un conjunto de códigos de acceso para :
    - Acceder a los sistemas de comunicación
    - Acceso a su pc

- Acceso a su teléfono
- Acceso a los equipos de impresión
- Acceso a los servidores
- Acceso a las aplicaciones
- Acceso a determinados ambientes
- Acceso a determinados casilleros
- Acceso a los servidores
- Acceso a las Bases de Datos
- Acceso a los ambientes de desarrollo
- Acceso a los documentos

3. Existen horarios de acceso definidos para cada tipo de personal. Para un acceso en horarios fuera de los definidos es necesario una autorización indicando el los días, horas y la intervención a realizar.
4. Existe un sistema de video vigilancia en los diferentes departamentos de la empresa y en las dos sedes. Estos videos son monitoreados en permanencia por el personal de seguridad. Esto videos son grabados y el registro de estos son almacenados.
5. Existe un sistema de detectores de presencia y alarmas activado en horarios determinados y en espacios determinados. Este sistema esta conectado a una central de alarmas y la policía.

2. 2 Objetivos

Objetivo General

Definir un plan director de seguridad de la información que defina los lineamientos generales que la empresa A2 debe seguir con miras a garantizar la protección y el buen uso de la información y los sistemas de información que la empresa utiliza.

Objetivos específicos

- Crear y promover la cultura de seguridad dentro de la empresa
- Identificar el nivel de seguridad existente en los sistemas, servicios y aplicaciones en el manejo de la información.
- Definir los roles, las responsabilidades en materia de seguridad para todo el personal que este llamado a trabajar con la información de la empresa
- Identificar los riesgos a los cuales están expuestos los activos de la empresa
- Definir los controles necesarios
- Definir y planificar los planes de acción a realizar teniendo como base referencia el nivel de seguridad actual y el nivel de seguridad al que se desea llegar.
- Definir directrices en materia de la seguridad de la información
- Implantar y hacer un seguimiento del plan de seguridad definido

- Garantizar la confidencialidad, integridad, disponibilidad y confiabilidad de la información y los sistemas de información que maneja la empresa.

2.3 Plan diferencial

Si bien la empresa tiene definidas medidas de seguridad establecidas, estas no están definidas dentro de un plan y no están siendo aplicadas a toda la empresa.

Con el propósito de conocer el estado actual de la organización con respecto a la seguridad de la Información, se hace un análisis diferencial de los diferentes controles con respecto a la normas ISO27001:2013 y ISO27002. Este análisis contrasta el estado actual de la implementación de la seguridad de la empresa con las normas referidas como guías.

Se utiliza el modelo CMM para conocer el estado de madurez y poder identificar mejores practicas necesarias para mejorar los procesos.

A continuación se presenta la tabla con los niveles del modelo CMM que serán utilizados para este análisis.

Grupos de practicas del CMM			
Nivel	**%**	**Significado**	**Descripción**
N5	100%	Optimizado	Las prácticas de base están mejorando continuamente
N4	95%	Administrado	Las prácticas básicas son controladas cuantitativamente
N3	90%	Definido	Las prácticas básicas están bien definidas
N2	50%	Repetible	Las prácticas de base se planifican y rastrean
N1	10%	Inicial	Las prácticas básicas se realizan de manera informal
N0	0%	Ninguno	No existen practicas o procesos básicos.

A continuación se presenta el estado de madurez del SGSI de la empresa con respecto a los requisitos establecidos en la norma 27001:2013.

No	**Requisitos**	**Estado**
4	Contexto de la organización	55%
5	Liderazgo	43%
6	Planificación	50%
7	Apoyo	58%
8	Operación	50%
9	Evaluación de	43%

	desempeño	
10	Mejora	50%
	Nivel de madurez del SGSI	**50%**

Como se puede observar de los resultados, se confirma que si bien la empresa tiene practicas de seguridad en marcha y corresponden a los diferentes requisitos de la norma, el estado de madurez necesita mejorarse. El estado de madurez actual de la empresa de 50% corresponde al nivel repetible del modelo CMM.

La tabla completa del análisis con respecto a la norma 27001:2013 puede ser consultado en el ANEXO I.

Para el análisis con referencia a la norma 27002:2013 y con el propósito de realizar estimaciones sobre el estado de cumplimiento de los distintos dominios se consideran aspectos adicionales que se evalúan para cada uno de los controles.

Los aspectos adicionales se especifican en la tabla que sigue:

N°	Aspectos a evaluar
1	Exploración
2	Reconocimiento
3	Documentación
4	Implantación
5	Evaluación
6	Mejoramiento

A continuación se presenta el estado de madurez del cumplimiento de los objetivos de control del SGSI de la empresa con respecto a la norma ISO 27002:2013.

Control	Cumplimento
5 POLÍTICA DE SEGURIDAD	50%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	46%
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	57%
8. GESTIÓN DE ACTIVOS	61%
9. CONTROL DE ACCESOS	65%
10. CRIPTOGRAFÍA	65%
11. SEGURIDAD FÍSICA DEL ENTORNO	72%
12. SEGURIDAD DE LAS OPERACIONES	68%
13. SEGURIDAD DE LAS COMUNICACIONES	58%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	65%

15. RELACIONES CON PROVEEDORES	64%
16 GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	64%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	68%
18. CUMPLIMIENTO	73%
NIVEL DE CUMPLIMIENTO GENERAL	63%

Como se puede observar los resultados en la tabla se constata que el porcentaje de cumplimiento es del 63%. Tomando como referencia la norma el nivel general de cumplimiento de los diferentes controles es Repetible dentro del modelo CMM. Se confirma que los controles de la empresa son de base, se planifican y se rastrean. El detalle de los diferentes controles se puede consultar en el ANEXO I.

El objetivo de la empresa a mediano plazo es llegar al nivel definido dentro de los niveles del CMM.

Esta grafica muestra los % de cumplimiento actuales con respecto a la norma ISO/IEC27002:2013.

3 Fase 2: Gestión Documental

3.1 Introducción

El Sistema de Gestión de Seguridad de la Información se apoya en un cuerpo documental para el cumplimiento normativo ISO/IEC 27001:2013. La existencia de este grupo de documentos constituyen requisitos imprescindibles para certificar que el SGSI funciona correctamente. Los documentos básicos para la implementación de un SGSI se detallan a continuación.

3.2 Política de Seguridad

Es el conjunto de normativas internas por las cuales se rige el manejo seguro de la información de la empresa. Siendo el propósito final de esta política la protección de los activos de información ante las diferentes amenazas (internas o externas).

Este documento constituye la base de las buenas practicas en materia de seguridad de la información buscando garantizar la confidencialidad, la integridad y la disponibilidad de la información. Los aspectos que cubre son los relativos al acceso de la información, el uso de recursos de la organización, comportamiento en caso de incidentes de seguridad, etc.

Es responsabilidad de la dirección la creación, aprobación, difusión, aplicación y revisión de las normativa de la empresa.

Todo el personal de la empresa debe tener conocimiento de esta normativa, aplicar y velar por el cumplimiento de la misma.

El documento de la política de seguridad se encuentra en el ANEXO II.

3.3 Procedimiento de Auditorias Internas

Documento que incluye la planificación de las auditorias que se llevaran a cabo durante la vigencia de la certificación (una vez que se obtenga), los requisitos que se establecerán a los auditores internos y se definirá el modelo de auditoria.

El documento del procedimiento de la auditoria interna se encuentra en el ANEXO III.

3.4 Gestión de Indicadores

En este documento se detallan los indicadores que va a utilizar la empresa para controlar el funcionamiento de las medidas de seguridad de la información que se van a implantar.

El documento con la tabla de indicadores se encuentra en el ANEXO IV.

3.5 Declaración de aplicabilidad

La declaración de la aplicabilidad recoge los controles especificados en la norma ISO/IEC 27002:2013 y especifica la aplicabilidad en la empresa A2.

La tabla de la declaración de la aplicabilidad se encuentra en el ANEXO V, la misma que además especifica las implementaciones actuales que tiene la empresa con referencia a los controles.

3.6 Procedimiento Revisión por Dirección

La Dirección de la organización debe realizar revisiones anuales de las cuestiones mas importantes que han sucedido con relación al Sistema de Gestión de la Seguridad de la Información. Para esta revisión la norma iso27001 define los puntos de entrada como los puntos de salida de estas revisiones.

El documento que incluye el procedimiento de Revisión se encuentra en el ANEXO VI.

3.7 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.

La descripción de los roles y responsabilidades del equipo mencionado se encuentran detalladas en el ANEXO VII.

3.8 Metodología de análisis de Riesgos

La metodología de análisis de riesgos establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

La metodología a usar en el análisis de riesgos es Magerit v3.0. Se trata de una metodología muy extendida y probada, que tiene la ventaja de expresar sus resultados en términos cuantitativos o cualitativos, lo que facilita la toma de decisiones.

La metodología a utilizar se encuentra descrita en el ANEXO VIII.

4 Fase 3: Análisis de Riesgos

4.1 Introducción

El análisis de riesgos es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

El análisis de riesgo es la primera etapa hacia la consecución del plan implementación de un SGSI,

El análisis de riesgos que sigue a continuación abarca las siguientes etapas:

1. Inventario de Activos
2. Valoración de Activos
3. Análisis de Amenazas
4. Impacto potencial
5. Impacto de Riesgo Aceptable y riesgo Residual

4.2 Inventario de activos

Se considera activo a todo aquello que tiene un valor para la organización y por lo tanto requiere de su protección.

Basados en metodología MAGERIT la clasificación de activos se la realiza de acuerdo a los siguientes ámbitos:

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

A continuación en las tablas siguientes se muestran el inventario de activos de la empresa de acuerdo a los ámbitos mencionados.

[S] Software Aplicaciones Informáticas

ID	Nombre	Activo	Propietario
[SW.1]	CNS	Aplicación de gestión de datos clientes	Dirección operaciones
[SW.2]	EXX	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones	Dirección operaciones
[SW.3]	XTR	Aplicación de gestión de los datos personales de los empleados de la empresa	Dirección RRHH
[SW.4]	BND	Aplicación de gestión de contratos de los clientes individuales	Dirección operaciones
[SW.5]	ULT	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas	Dirección operaciones
[SW.6]	GAN	Aplicación de gestión de contratos empresariales – seguros de grupo	Dirección operaciones
[SW.7]	FIN	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos	Dirección Finanzas
[SW.8]	PEJ	Aplicación contable de la empresa	Dirección Finanzas
[SW.9]	FSRD	Servidor de documentos de desarrollo	Dirección operaciones/legal
[SW.10]	FSRT	Servidor de documentos en TST	Dirección IT
[SW.11]	FSRI	Servidor de documentos en INT	Dirección IT
[SW.12]	FSRP	Servidor de documentos en PRD	Dirección Operaciones/legal
[SW.13]	SDV	Servidor de aplicaciones de desarrollo	Dirección IT
[SW.14]	SDT	Servidor de aplicaciones de test	Dirección IT
[SW.15]	SDIB	Servidor de aplicaciones de integración	Dirección operaciones/legal
[SW.16]	SDPB	Servidor de aplicaciones de producción	Dirección operaciones/legal
[SW.17]	SDBD	SGBD Oracle en desarrollo	Dirección IT
[SW.18]	SDBT	SGBD Oracle en test	Dirección IT
[SW.19]	SDBI	SGBD Oracle en integración	Dirección operaciones
[SW.20]	SDBP	SGBD Oracle en producción	Dirección operaciones

[HW] Hardware

ID	Nombre	Activo	
[HW.1]	SFI	Servidor de aplicaciones internas/finanzas/admini/compta	Dirección IT
[HW.2]	SER	Servidores DNS	Dirección IT
[HW.3]	SDB	Servidores DB Oracle prod	Dirección IT
[HW.4]	SDB	Servidores DB Oracle dev	Dirección IT
[HW.5]	SDB	Servidores DB Oracle test	Dirección IT
[HW.6]	SDB	Servidores DB Oracle int	Dirección IT
[HW.7]	SEE	Servidores de e-comerce	Dirección IT
[HW.8]	ROU	Routers	Dirección IT
[HW.9]	SCO	Servidores de correo	Dirección IT
[HW.10]	SDE	Servidores de Desarrollo	Dirección IT

[HW.11]	SDT	Servidores de Test	Dirección IT
[HW.12]	SDU	Servidores de Integración	Dirección IT
[HW.13]	SPO	Servidores de Producción	Dirección IT
[HW.14]	PCP	PC Portables	Dirección IT
[HW.15]	PCF	PC de escritorio fijas	Dirección IT
[HW.16]	TAB	Tabletas	Dirección IT
[HW.17]	TFI	Teléfonos fijos	Dirección IT
[HW.18]	TMO	Teléfonos móviles	Dirección IT
[HW.19]	VPN	Dispositivos de conexión VPN	Dirección IT
[HW.20]	RAC	Rack de comunicaciones	Dirección IT
[HW.21]	SWI	Switchs	Dirección IT
[HW.22]	FIR	Firewalls	Dirección IT
[HW.23]	WIF	Sistema Wifi	Dirección IT
[HW.24]	CAB	Cableado de la red	Dirección IT
[HW.25]	CAM	Cámaras de vigilancia	Dirección IT
[HW.26]	WSR	Servidor de documentos	Dirección IT
[HW.27]	BSR	Servidores de copias de seguridad	Dirección IT
[HW.28]	IMP	Multiservidores de impresión/scanner/fotocopias	Dirección IT

[I]Instalaciones			
ID	**Nombre**	**Activo**	
[I.1]	CPD	Centro de procesamiento de datos	Dirección IT
[I.2]	REU	Salas de Reuniones	Dirección Operaciones
[I.3]	OPE	Puestos de trabajo del personal – open spaces	Dirección RG
[I.4]	AQU	Puestos de trabajo bajo seguro	Dirección IT
[I.5]	OFI	Oficinas de los directivos	Dirección RH
[I.6]	PRI	Salas de impresión	Dirección IT
[I.7]	UNI	Unidades de apoyo a los servicios	Dirección Operaciones
[I.8]	RAC	Espacios de almacenamiento de los racks	Dirección IT
[I.9]	ARM	Espacio de almacenamiento de documentos papel seguros	Dirección Operaciones

[D] Datos/Información			
ID	**Nombre**	**Activo**	
[D.1]	CFC	Código fuentes aplicaciones de gestión de contratos	Dirección operaciones
[D.2]	CFU	Código fuente aplicaciones de gestión de usuarios	Dirección Operaciones
[D.3]	CFE	Código fuente aplicaciones de gestión de datos de empleados	Dirección Operaciones
[D.4]	CFX	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones	Dirección operaciones
[D.5]	DCI	Datos de clientes individuales	Dirección operaciones
[D.6]	DCE	Datos de clientes empresariales	Dirección

			operaciones
[D.7]	DCF	Datos de clientes independientes	Dirección operaciones
[D.8]	DEM	Datos de los empleados de la empresa	Dirección RRHH
[D.9]	DAC	Datos de acceso a las aplicaciones (roles y responsabilidades)	Dirección operaciones
[D.10]	DCC	Documentos de clientes	Dirección operaciones
[D.11]	DEC	Documentos de empleados	Dirección RRHH
[D.12]	DOC	Documentos otros	Dirección operaciones
[D.13]	DSL	Datos de soporte y licencias	Dirección IT
[D.14]	LOG	Log de servidores y log de clientes	Dirección IT
[D.15]	BKP	Backup de la DB de usuarios	Dirección IT
[D.16]	DPA	Documentos en papel (contratos)	Dirección operaciones
[D.17]	BKP	Backup código fuente	Dirección IT
[D.18]	BKDB	Backup de la DB Clientes	Dirección operaciones
[D.19]	BKE	Backup de la DB empleados	Dirección IT
[D.20]	BKC	Datos de configuración	operaciones

[COM]: Redes de comunicaciones			
ID	**Nombre**	**Activo**	**Propietario**
[COM.1]	INT	Internet	Dirección IT
[COM.2]	WIF	Red inalámbrica	Dirección IT
[COM.3]	CAB	RED telefónica	Dirección IT
[COM.4]	ETH	RED telecomunicaciones	Dirección IT
[COM.5]	TMO	Telefonía móvil	Dirección IT
[COM.6]	LAN	Red Local	Dirección IT
[COM.7]	CEL	Cableado eléctrico	Dirección IT

[S] Servicios			
ID	**Nombre**	**Activo**	**Propietario**
[S.1]	INT	Servicio Web	Dirección operaciones
[S.2]	CAB	Servicio de aplicaciones	Dirección IT
[S.3]	SEA	Servicios de archivos	Dirección operaciones
[S.4]	SED	Servicios de documentos	Dirección operaciones
[S.5]	SDN	Servicios DNS	Dirección IT
[S.6]	SEE	Servicios email	Dirección IT
[S.7]	SEC	Servicio comunicaciones	Dirección Comercial
[S.8]	POE	Portal interno	Dirección operaciones
[S.9]	POI	Portal Externo	Dirección Comercial

[AUX] Equipamiento Auxiliar			
ID	Nombre	Activo	**Propietario**
[AUX.1]	LOC	Lockers	Dirección RG
[AUX.2]	MUL	Multiprinters	Dirección Comercial
[AUX.3]	REC	Recursos varios (material de escritorio, maletas, …)	Dirección RG
[AUX.4]	TVE	Televisores	Dirección IT
[AUX.5]	EQS	Equipos de sonido y proyección	Dirección IT
[AUX.6]	PAN	Pantallas	Dirección IT
[AUX.7]	CAB	Electricidad	Dirección IT
[AUX.8]	MOB	Mobiliario	Dirección RH

[P] Personal			
ID	**Nombre**	**Activo**	**Propietario**
[P.1]	CEO	Director General	Dirección General
[P.2]	CITO	Director IT	Dirección IT
[P.3]	COO	Director operaciones	Dirección operaciones
[P.4]	CRH	Director de recursos humanos	Dirección de recursos humanos
[P.4]	CRO	Directos Riesgos	Dirección Riesgos
[P.5]	CFI	Director Finanzas	Dirección Finanzas
[P.6]	DMA	Director Comercialización y ventas	Dirección Comercialización
[P.7]	EQD	Personal de desarrollo de las aplicaciones	Dirección IT
[P.8]	GQD	Gestionaros de contratos/Business Experts	Dirección Operaciones
[P.9]	EQO	Personal RH	Dirección RH
[P.10]	ADA	Administradores de aplicaciones	Dirección IT
[P.11]	TSB	Técnicos de soporte business	Dirección Operaciones
[P.12]	AGV	Agentes de ventas	Dirección Operaciones
[P.13]	PMA	Personal Comercial	Dirección Comercial
[P.14]	PFI	Personal de Finanzas	Personal de Finanzas
[P.15]	PIN	Personal Infraestructura	Dirección IT
[P.16]	PRI	Personal Risks	Dirección Risks
[P.17]	ADS	Administradores de sistemas	Dirección IT
[P.18]	PSI	Personal de soporte IT	Dirección IT

4.3 Valoración de los activos

La valoración de los activos se la realizara considerando el valor que tiene para la empresa así como también la dependencia del activo con otros activos, pues los activos se encuentran dentro de una jerarquía. La escala de valoración que se utilizara es Muy Alta, Alta, Media, Baja y Muy Baja.

Se dice que un 'activo superior' depende de 'otro inferior' cuando las necesidades de seguridad del activo superior se reflejan en las necesidades de seguridad del activo inferior (cuando la materialización de una amenaza en el

activo inferior tiene como consecuencia un perjuicio sobre el activo superior). De ahí la importancia de conocer la dependencia de los activos para poder valorar los activos.

De manera general podemos resumir la dependencia entre activos como sigue:

1. El Hardware [HW] depende de las instalaciones [I], elementos de la RED [COM] y de componentes auxiliares como las electricidad [AUX]
2. EL Software [SW] depende del Hardware [HW]
3. Los Datos [D] dependen del Hardware [HW] y del Software [SW]
4. Las Comunicaciones [COM] dependen del Hardware [HW], de las Instalaciones [I] y de componentes auxiliares [AUX]
5. Los Servicios [S] dependen del Hardware [HW], del Software [SW], de la red de Comunicaciones [COM] y las instalaciones eléctricas [I] o fuentes de poder.
6. Soportes de información [SI] dependen de instalaciones [I] et probablemente de algún [AUX] dependiendo del activo con el cual se va a trabajar.
7. Los Auxiliares [AUX] depende de las Instalaciones [I], del Hardware [HW] y otros [AUX].
8. Personal [P] y las Instalaciones [I] no tienen dependencias.

4.4 Dimensiones de seguridad

Las dimensiones de la seguridad son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo y que es independiente de otras facetas. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Las 5 dimensiones son las siguientes:

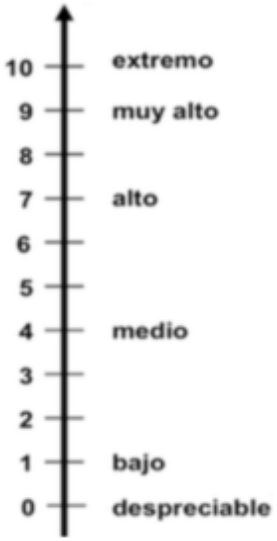
[A] Autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)
[C] Confidencialidad de la información

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
[I] Integridad de la información
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
[D] Disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios .
[T] Trazabilidad del uso del servicio
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

Usaremos estas dimensiones en el proceso de valoración de los activos lo que permitirá a posteriori valorar el impacto de la materialización de una amenaza sobre el activo en cuestión.

Para la valoración de las dimensiones se ha elegido una escala detallada de diez valores, dejando el valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo).

Para el proceso de valoración se utiliza una tabla simplificada de 6 niveles que se detalla a continuación y que esta dentro de la escala de valores definida.



Valor			Criterio
10	E	Extremo	Daño Extremadamente Grave
9	MA	Muy Alto	Daño Muy Grave
6-8	A	Alto	Daño Grave
3-5	M	Medio	Daño Importante
1-2	MB	Bajo	Daño Menor
0	D	Despreciable	Irrelevante a efectos prácticos.

La tabla de activos con sus valoraciones se encuentra en el ANEXO IX.

4.5 Análisis de Amenazas

Los activos están expuestos a amenazas que pueden afectar diferentes aspectos de la seguridad.

Magerit clasifica las amenazas en 4 grandes grupos:

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

La tabla detallada de las amenazas se encuentra en el ANEXO XIII.

La valoración de la influencia de la amenaza en el valor del activo se la realiza en dos sentidos:

- degradación: cuán perjudicado resultaría el valor del activo y
- la probabilidad: cuán probable o improbable es que se materialice la amenaza

La frecuencia de la ocurrencia de una amenaza se la va a medir de acuerdo a la siguiente escala de valores:

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

Para la valoración del impacto que la ocurrencia de una amenaza produciría sobre las dimensiones de seguridad de un activo utilizaremos 5 niveles posibles de impacto como se muestra en la tabla siguiente:

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

En el ANEXO X se tiene la tabla que muestra la valoración de las amenazas que afectan a los diferentes activos de la empresa, detallando la frecuencia de ocurrencia de cada amenaza y el impacto que tendría la ocurrencia de cada amenaza dentro de la 5 dimensiones de seguridad del activo.

La siguiente tabla es un resumen de los impactos máximos de las diferentes amenazas para las 5 dimensiones de seguridad de los activos.

Activo	Impacto				
	A	C	I	D	T
[D] Datos- Información	100%	100%	100%	100%	100%
[S] Servicios	75%	75%	75%	100%	100%
[SW] Software	75%	75%	75%	100%	
[HW] Hardware		100%	50%	100%	
[AUX] Equipo Auxiliar		50%	75%	100%	
[COM]: Redes		100%	50%	100%	
[I] Instalaciones		20%	20%	100%	
[P] Personal		75%	20%	100%	

4.6 Impacto Potencial

Partiendo del análisis de activos se puede determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Este es un dato relevante que permitirá priorizar el plan de acción y al mismo tiempo evaluar como se modifica este valor cuando se aplican contramedidas.

El impacto potencial se calcula como sigue:

IMPACTO POTENCIAL = VALOR DEL ACTIVO * VALOR DEL IMPACTO DE LA AMENAZA

La tabla completa de activos con el calculo del impacto potencial se encuentra en el ANEXO XI.

4.7 Nivel de Riesgo Aceptable y nivel de Riesgo Residual

El riesgo será mayor cuanto mayor sea el impacto y mayor la frecuencia de ocurrencia.

Partiendo del hecho que no todos los riesgos pueden erradicarse, es importante y necesario definir un nivel a partir del cual se decida asumir o no asumir el riesgo. El nivel a partir del cual se van a aplicar controles para reducir los riesgos.

Los riesgos residuales son aquellos que pese a todas las medidas de control aplicadas permanecen.

El siguiente paso es calcular el riesgo para cada una de las dimensiones de seguridad.

RIESGO= IMPACTO POTENCIAL * FRECUENCIA

Para la estimación del riesgo se utilizan una escala cualitativa para modelar el impacto, la frecuencia y el Riesgo mismo.

Escalas		
Impacto	Frecuencia	Riesgo
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Así mismo se pueden combinar el impacto y la frecuencia para calcular el riesgo.

Los niveles de riesgo se pueden resumir en el siguiente cuadro:

RIESGO		PROBABILIDAD				
		MB (0,002)	B (0,005)	M (0,016)	A (0,071)	MA (1)
IMPACTO	MA (10)	A	MA	MA	MA	MA
	A (7-9)	M	A	A	MA	MA
	M (4-6)	B	M	M	A	A
	B (2-3)	MB	B	B	M	M
	MB (1)	MB	MB	MB	B	B

La tabla de valoración completa de los riesgos se encuentra en el ANEXO XII.

Estos resultados obtenidos nos dan una visión clara sobre el estado actual de la seguridad de los activos de la empresa .

La empresa ha establecido 5 niveles de riesgo para su tratamiento (MB, B, M, A, MA). Los niveles de riesgo tolerables y aceptables son los niveles MB, B, y M.

Los niveles de riesgo no tolerables son los niveles A y MA. Siendo los niveles MA prioritarios para su tratamiento.

4.8 Resultados

A continuación se resume los resultados del análisis de riesgos y se agrupan los activos por niveles de tratamiento.

Tabla de tratamiento de riesgos críticos

ID	Activo	Riesgo
[D.1]	Código fuentes aplicaciones de gestión de contratos	MA
[D.2]	Código fuente aplicaciones de gestión de usuarios	
[D.3]	Código fuente aplicaciones de gestión de datos de empleados	
[D.4]	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones	
[D.14]	Log de servidores y log de clientes	
[D.5]	Datos de clientes individuales	
[D.6]	Datos de clientes empresariales	
[D.7]	Datos de clientes independientes	
[D.8]	Datos de los empleados de la empresa	
[P.1]	Director General	
[P.2]	Director IT	
[P.3]	Director operaciones	
[P.5]	Director Finanzas	
[P.7]	Personal de desarrollo de las aplicaciones	
[P.8]	Gestionaros de contratos/Business Experto	
[P.10]	Administrador de la aplicación	

[P.11]	Técnicos de soporte Business	
[P.14]	Personal Finanzas	
[P.15]	Personal Infraestructura	
[P.17]	Administradores de sistemas	

ID	Activo	Riesgo
[SW.1]	Aplicación de gestión de datos clientes	
[SW.2]	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones	
[SW.3]	Aplicación de gestión de los datos personales de los empleados de la empresa	
[SW.4]	Aplicación de gestión de contratos de los clientes individuales	
[SW.5]	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas	
[SW.6]	Aplicación de gestión de contratos empresariales – seguros de grupo	
[SW.7]	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos	
[SW.8]	Aplicación contable de la empresa	
[SW.11]	Servidor de documentos en INT	
[SW.12]	Servidor de documentos en PRD	
[SW.16]	Servidor de aplicaciones de producción	
[SW.20]	SGBD Oracle en producción	
[HW.1]	Servidor de aplicaciones internas/finanzas/admini/compta	
[HW.2]	Servidores DNS	
[HW.3]	Servidores DB Oracle prod	
[HW.5]	Servidores DB Oracle test	
[HW.6]	Servidores DB Oracle int	
[HW.7]	Servidores de e-comerce	
[HW.8]	Routers	
[HW.9]	Servidores de correo	
[HW.12]	Servidores de Integración	
[HW.13]	Servidores de Producción	
[HW.14]	PC Portables	
[HW.19]	Dispositivos de conexión VPN	
[HW.20]	Rack de comunicaciones	A
[HW.21]	Switchs	
[HW.23]	Sistema Wifi	
[HW.24]	Cableado de la red	
[HW.26]	Servidor de documentos	
[HW.27]	Servidor de copias de seguridad	
[I.1]	Centro de procesamiento de datos	
[I.3]	Puestos de trabajo del personal – open spaces	
[D.9]	Datos de acceso a las aplicaciones (roles y responsabilidades)	
[D.10]	Documentos de clientes	

[D.11]	Documentos de empleados	
[D.12]	Documentos otros	
[D.13]	Datos de soporte y licencias	
[D.15]	Backup de DB users	
[D.16]	Documentos en papel (contratos)	
[D.17]	Backup código fuente	
[D.18]	Backuo de DB Clientes	
[D.19]	Backup DB empleados	
[D.20]	Datos de configuración	
[COM.1]	Internet	
[COM.2]	Red inalámbrica	
[COM.4]	Cableado telecomunicaciones	
[COM.6]	Red Local	
[COM.7]	Cableado electrico	
[S.1]	Servicio Web	
[S.2]	Servicio de aplicaciones	
[S.3]	Servicios de archivos	
[S.4]	Servicios de documentos	
[S.5]	Servicios DNS	
[S.7]	Servicio comunicaciones	
[S.9]	Portal Externo	
[P.12]	Agentes de ventas	
[P.13]	Personal Comercial	
[P.16]	Personal Risks	
[P.18]	Personal de soporte IT	

ID	Activo	Riesgo
[SW.9]	Servidor de documentos de desarrollo	
[SW.10]	Servidor de documentos en TST	
[SW.13]	Servidor de aplicaciones de desarrollo	
[SW.14]	Servidor de aplicaciones de test	
[SW.15]	Servidor de aplicaciones de integración	
[SW.17]	SGBD Oracle en desarrollo	
[SW.18]	SGBD Oracle en test	
[SW.19]	SGBD Oracle en integración	
[HW.4]	Servidores DB Oracle dev	
[HW.7]	Servidores de e-comerce	
[HW.10]	Servidores de Desarrollo	
[HW.11]	Servidores de Test	
[HW.15]	PC de escritorio fijas	
[HW.16]	Tabletas	
[HW.22]	Firewalls	M

[HW.25]	Cámaras de vigilancia	
[HW.28]	Multiservidores de impresión/scanner/fotocopias	
[I.2]	Salas de Reuniones	
[I.4]	Puestos de trabajo bajo seguro	
[I.5]	Oficinas de los directivos	
[COM.3]	RED telefónica	
[COM.5]	Telefonía móvil	
[S.6]	Servicios email	
[S.8]	Portal interno	
[AUX.1]	Lockers	
[AUX.2]	Multiprinters	
[AUX.8]	Mobiliario	
[P.4]	Director de recursos humanos	
[P.4]	Directos Riesgos	
[P.6]	Director Marketing y ventas	
[P.9]	Personal RH	

	Activo	Riesgo
[AUX.3]	Recursos varios (material de escritorio, maletas, …)	
[AUX.4]	Televisores	
[AUX.5]	Equipos de sonido y proyección	
[AUX.6]	Pantallas	
[I.6]	Salas de impresión	
[I.7]	Unidades de apoyo a los servicios	
[HW.17]	Teléfonos fijos	B
[HW.18]	Teléfonos móviles	

5. Fase 4: Propuesta de Proyectos

5.1. Introducción

Partiendo de los resultados obtenidos del capitulo anterior se conoce los riesgos a los cuales está expuesta la empresa. En este capitulo se plantean proyectos que buscan mejorar el estado de la seguridad de la información de la empresa.

El Plan de Seguridad que se plantea no sólo busca la mejora relacionada con la gestión de la seguridad, sino también posibles beneficios colaterales como la optimización de los recursos, mejoras en la gestión de procesos y las tecnologías presentes en la organización analizada.

5.2 Proyectos propuestos

El objetivo de los proyectos que se plantean a continuación es mitigar los riesgos identificados.

Se han definido 10 proyectos que a ser implementados a corto, a mediano y a largo plazo.

ID	Nombre	Plazos
PR001	Políticas de seguridad de la Información	**A corto plazo**
PR001	Plan de Continuidad del Negocio	
PR003	Plan de Formación y concientización	
PR004	Políticas de control de acceso y de acceso a la red y los servicios de red	
PR005	Gestión del acceso del usuario	
PR002	Plan de continuidad del Negocio	**A mediano Plazo**
PR006	Control de acceso al sistema y aplicaciones	
PR007	Revisión del SGSI	
PR008	Mejora en la gestión de Recursos Humanos	**A largo plazo**
PR009	2F autenticación	
PR010	Clasificación de la Información	
PR011	Copias de Respaldo	

Id del proyecto	**PR001**
Nombre del proyecto	Políticas de seguridad de la Información

Objetivo	Actualizar el documento de políticas de seguridad. Mejorar el soporte de la gestión de la seguridad de la información.
Responsable	Responsable de la seguridad
Descripción	Este proyecto busca actualizar las políticas existentes dentro de la organización en función a los cambios tecnológicos, cambios en la empresa y/o nuevos requerimientos no tratados y necesidades en materia de seguridad. Se busca identificar políticas obsoletas, actualizar y definir nuevas políticas necesarias para el manejo seguro de la información en las condiciones actuales de la organización. Este documento debe ser aprobado por la dirección. Este documento debe ser implantado inmediatamente. Este documento debe ser revisado anualmente.
Activos Afectados	Todos los activos
Dominios ISO/IEC 27002:2013	A.5
Dimensiones de seguridad afectadas	ACIDT
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información.
Duración	40 días
Recursos	Responsable de la Seguridad Director General Directivos de la empresa Propietarios de la Información y los Sistemas
Costos Estimados	€20000.-

Id del proyecto	**PR002**
Nombre del proyecto	Plan de continuidad del Negocio
Objetivo	Definir un plan que de respuestas rápidas y agiles ante situaciones que no se han podido evitar pese a las diferentes medidas de seguridad implementadas.
Responsable	Responsable de la seguridad
Descripción	Este proyecto busca desarrollar un plan de actuación que es destinado a mitigar el impacto sobre la información y los procesos del negocio cuando los riesgos se concretizan. Este plan debe asegurar la continuidad del negocio y evitar que las actividades del core business de la empresa sean interrumpidas o si lo fueran que estas puedan ser restablecidas en plazos razonables. Este plan debe especificar las medidas técnicas, humanas

	y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía Este plan de continuidad será revisado anualmente.
Activos Afectados	Instalaciones de los equipos. Hardware: Los equipos de producción Software: Las aplicaciones de gestión de contratos implementadas en producción Datos: Las bases de datos en producción para las aplicaciones de gestión de contratos. Redes: Las redes internas y externas Personal: Director general, Director IT, Director de Operaciones, y personal de gestión del Core Business.
Dominios ISO/IEC 27002:2013	A.17.1
Dimensiones de seguridad afectadas	Disponibilidad
Riesgos mitigados	Disponibilidad de la información, de los servicios y la infraestructura
Duración	40 días
Recursos Humanos	Responsable de la seguridad Director general Directores de Finanzas, Operaciones y IT Personal del core business
Costos Estimados	€30000

Id del proyecto	**PR003**
Nombre del proyecto	Plan de Formación y concientización
Objetivo	Actualizar e implementar el plan de formación del personal en materia de seguridad de la información
Responsable	Responsable de la seguridad
Descripción	Se actualiza el plan de formación y capacitación en materia de seguridad de la información. Este programa de formación está dirigido a todo el personal de la empresa (interno y externo) así como los contratistas. en función a los temas, las disponibilidades y necesidades de formación identificadas para los distintos miembros del personal. En este plan de formación están incluidos personal, interno y externo. Este programa de formación es obligatorio para todo el personal (interno y externo) y debe estar finalizado el año en curso.

	Este proyecto es recurrente anualmente. El plan de formación incluye dentro de su temario: - Seguridad del manejo de la información - Políticas de seguridad - Riesgos en materia de seguridad de la información - Procesos y procedimientos de seguridad - Uso correcto de la información, y los que medios que se disponen para su tratamiento - Infracciones - Incidentes de seguridad - Medidas de seguridad - Responsabilidades y su alcance - Proceso disciplinario - Reglamento interno - Leyes y normas
Activos Afectados	Todo el personal de la empresa
Dimensiones de seguridad afectadas	CID
Riesgos mitigados	Confidencialidad, Integridad y Disponibilidad de la información
Dominios ISO/IEC 27002:2013	A.7.2
Recursos	Responsable de la Seguridad Director General Director de Recursos Humanos Formadores
Tiempo	2 cursos de 4 horas por semana.
Costos Estimados	10000€

Id del proyecto	**PR004**
Nombre del proyecto	Políticas de control de acceso y de acceso a la red y los servicios de red
Objetivo	Revisar y Actualizar el documento de políticas de control de acceso a la información. Definir y actualizar las reglas de acceso a los diferentes activos, a las redes y los servicios en red.
Responsable	Responsable de la seguridad
Descripción	Este proyecto busca actualizar las políticas con referencia al control de acceso a la información dentro de la organización, así como del uso de las redes y los servicios en red.

	Estas políticas de control de acceso están basadas en los requerimientos del business de la empresa y la seguridad de la información requerida. El documento de la política deberá establecer las reglas de acceso, físicas y lógicas, para cada tipo de usuario. Definir los procedimientos que se van a utilizar para conceder privilegios de acceso y designar los responsables de los mismos Este proyecto busca disminuir el numero de accesos y conexiones no autorizadas e inseguras a la información, la red y/o servicios de red. Ser actualizada y revisada periódicamente.
Activos Afectados	Todos los activos
Dominios ISO/IEC 27002:2013	A.9.1
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información.
Tiempo	30 días
Costos Estimados	€20000

Id del proyecto	**PR005**
Nombre del proyecto	Gestión del acceso del usuario
Objetivo	Definir procesos y procedimientos formales para asegurar el acceso solo a los usuarios autorizados a los sistemas y los servicios.
Responsable	Responsable de la seguridad
Descripción	Este proyecto busca definir procesos y procedimientos formales para. - Registro y cancelación de los usuarios - Asignación de acceso de usuarios - Gestión de los privilegios - Gestión de las contraseñas de los usuarios - Revisión de los derechos de acceso
Activos Afectados	Todos los activos
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información
Dimensiones de seguridad afectadas	ACIDT
Dominios ISO/IEC 27002:2013	A.9.2
Recursos	Responsable de la Seguridad Directores Operaciones, IT

Tiempo	30 días
Costos Estimados	€20000

Id del proyecto	**PR006**
Nombre del proyecto	Control de acceso al sistema y aplicaciones
Objetivo	Evitar los accesos no autorizados a los sistemas y aplicaciones
Responsable	Responsable de la seguridad
Descripción	Este proyecto busca evitar los accesos no autorizados a los sistemas y las aplicaciones. Para ello se busca: - restringir el acceso a la información y a las funciones de las aplicaciones de acuerdo a las políticas de acceso definidas - Definir un procedimiento de control de inicio de sesión seguro cuando así se lo requiera - Definir un sistema des gestión de contraseñas interactivos y que generen contraseñas de calidad - Restringir y controlar los programas utilitarios que anulan el sistema y los controles de aplicación - Restringir el acceso a los códigos fuente de los programas
Activos Afectados	Datos Aplicaciones
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información
Dominios ISO/IEC 27002:2013	A.9.4.1 A.9.4.2 A.9.4.3 A.9.4.5 A.12.7
Indicadores	Restricción de acceso a la información Procedimiento de inicio de sesión seguro Sistema de gestión de contraseñas Control de acceso al código fuente de los programas
Recursos Humanos	Responsable de la seguridad Director IT Director de Operaciones,
Tiempo	30 días
Costos Estimados	€20000

Id del proyecto	**PR007**
Nombre del proyecto	**Revisión del SGSI**

Objetivo	Conocer es estado actual de la seguridad de la información en la empresa.
Responsable	Director general
Descripción	Se realizar una proceso de auditoria interna al SGSI de la empresa. Se busca determinar si los objetivos, los controles, los procesos y los procedimientos del SGSI están de acorde a los requisitos establecidos por la empresa en materia de seguridad de la información. Si están siendo implementados y mantenidos de manera eficaz. Este proceso se repite anualmente.
Activos Afectados	Todos los activos
Dominios ISO/IEC 27002:2013	A.18.2
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información
Duración	85 días
Recursos humanos	Responsable de la seguridad Auditor interno Personal a entrevistar
Costos Estimados	€ 20000

Id del proyecto	**PR008**
Nombre del proyecto	Mejora en la gestión de Recursos Humanos
Objetivo	Modificar y completar los procesos y procedimientos de la Gestión de RH
Responsable	Responsable RH
Descripción	Modificar y completar los procesos asociados a la seguridad ligada a los recursos humanos. El objetivo es que todos los empleados y proveedores de servicios apliquen la seguridad de la información, se responsabilicen del manejo de la información y estén sometidos a procesos disciplinarios en caso de infracciones. Se actualizaran los procesos en materia de seguridad para la contrataciones y los retiros del personal. Estos procesos deben ser revisados periódicamente.
Activos Afectados	Todos los activos
Dominios ISO/IEC 27002:2013	A.7 A.8.1.2

	A.18.1.2 A.18.1.4 A.13.2.4
Dimensiones de seguridad afectadas	ACD
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información
Duración	30 días
Recursos humanos	Responsable de la seguridad Responsable RH
Costos Estimados	€20000

Id del proyecto	**PR009**
Nombre del proyecto	2F autenticación
Objetivo	Reforzar la seguridad de acceso a las aplicaciones de la empresa
Responsable	Responsable de la seguridad
Descripción	Se va ha implementar el sistema de doble verificación en el proceso de autenticación de los usuarios al acceso a las principales aplicaciones como a los recursos de información críticos de la red. Se busca mejorar la seguridad durante el acceso y disminuir los accesos no autorizados.
Activos Afectados	Todas las aplicaciones y sistemas de información de la empresa
Dominios ISO/IEC 27002:2013	A.9.1.2 A.9.1.1
Dimensiones de seguridad afectadas	A.C.T
Riesgos mitigados	Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información
Duración	35 días
Recursos	Responsable de la Seguridad Director IT Personal IT con experiencia en 2F autenticación Usuarios para el proceso de tests
Costos Estimados	€50000.-

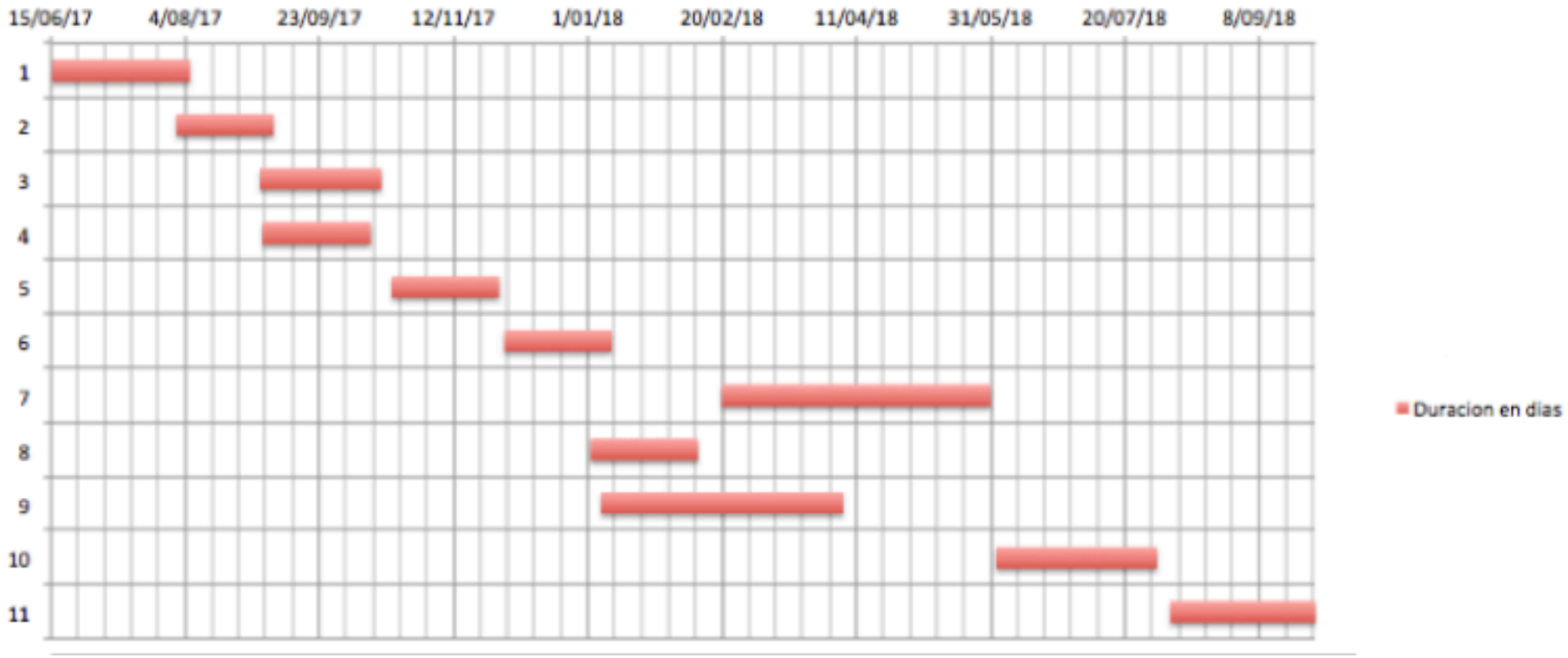
Id del proyecto	**PR010**
Nombre del proyecto	Clasificación de la Información
Objetivos	Clasificar y etiquetar la información. Asegurar que se aplique un nivel de protección adecuado a

	la información.
Responsable	Director de Operaciones
Descripción	Revisar la clasificación de la información en términos de los requisitos legales, valores críticos y sensibilidad para su divulgación y/o modificación. Se revisan, modifican y definen nuevos procedimientos para el etiquetado de la información. Verificar que el esquema de clasificación de la información permite comunicar las prioridades, necesidades de aplicación de medidas especiales de tratamiento y de definir un conjunto adecuado de niveles de protección.
Activos Afectados	Toda la Información Propietarios de la información
Dominios ISO/IEC 27002:2013	A.8.2 A.9.1.1
Dimensiones de seguridad afectadas	CDI
Riesgos mitigados	Confidencialidad, Integridad, Disponibilidad de la información.
Duración	55 días
Recursos	Responsable de la Seguridad Director de Operaciones Propietarios de la Información
Costos Estimados	€30000.-

Id del proyecto	**PR011**
Nombre del proyecto	Copias de Respaldo
Objetivo	Mejorar el grado de protección contra la perdida de los datos, mejorando el sistema de gestión de copias de respaldo y de recuperación.
Responsable	Director IT
Descripción	Se revisaran las políticas de backups existentes en la empresa. Se harán mejoras en el sistema que gestiona los backups y la recuperación de los datos e información. Se modifica y se aprueba la política de backups. Se implementa el sistema de backup. Se hace revisión de la política anualmente. Se realizan comprobaciones de los soportes de respaldo. Se realizan comprobaciones de los datos restaurados. Se hace una revisión de los resultados de los distintos procesos de backup y recuperación.
Activos Afectados	Bases de datos de los clientes Bases de datos de los empleados

	Códigos fuente de las aplicaciones Documentos de la empresa
Dominios ISO/IEC 27002:2013	A.12.3 A.17.1.2
Riesgos mitigados	Integridad y Disponibilidad de la información y los servicios de tratamiento de la información y comunicación.
Duración	40 días
Recursos	Responsable de la Seguridad Director IT
Costos Estimados	€30000.-

5.3 Planificación de los proyectos



5.4 Cumplimiento de los dominios después de la implantación de los proyectos

La implantación de los proyectos con miras a minimizar los riesgos sobre los activos ha afectado en la mejora del cumplimiento de ciertos dominios de la norma ISO/IEC27002:2013. Esto debido a la implementación de controles de la norma en los proyectos propuestos lo que incide en una mejora en los niveles de cumplimiento de ciertos dominios.

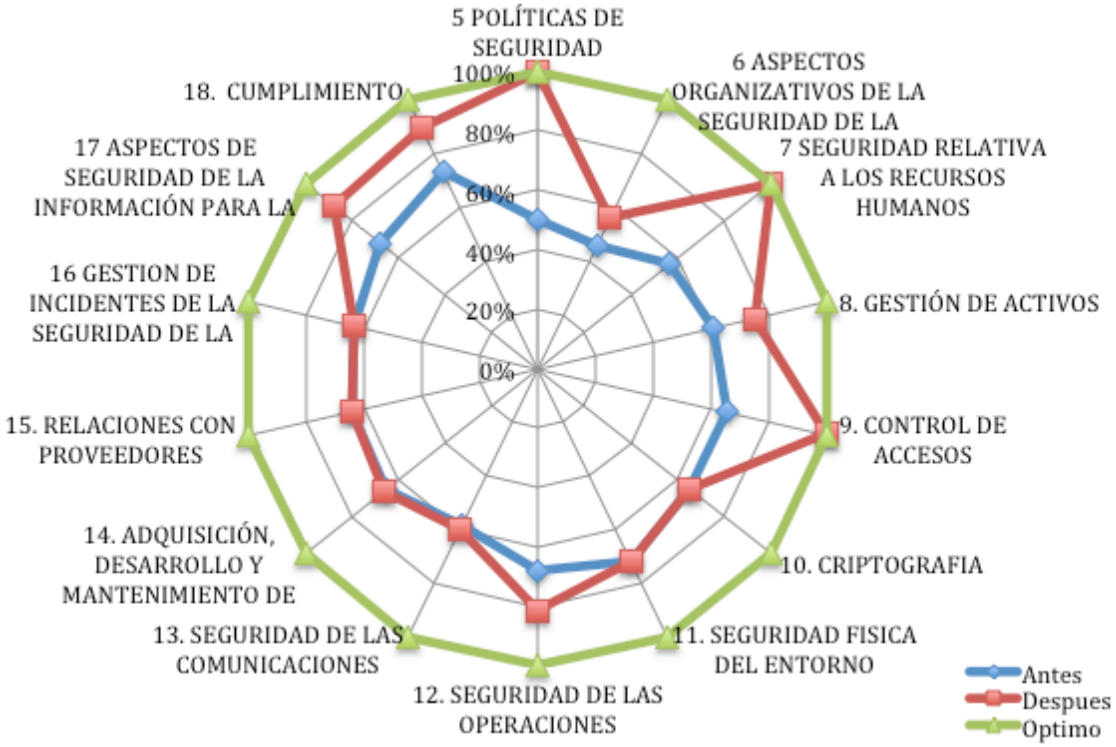
La siguiente tabla resume los niveles de cumplimiento para los diferentes dominios de la norma ISO/IEC27002:2013 una vez que los proyectos han sido implementados satisfactoriamente.

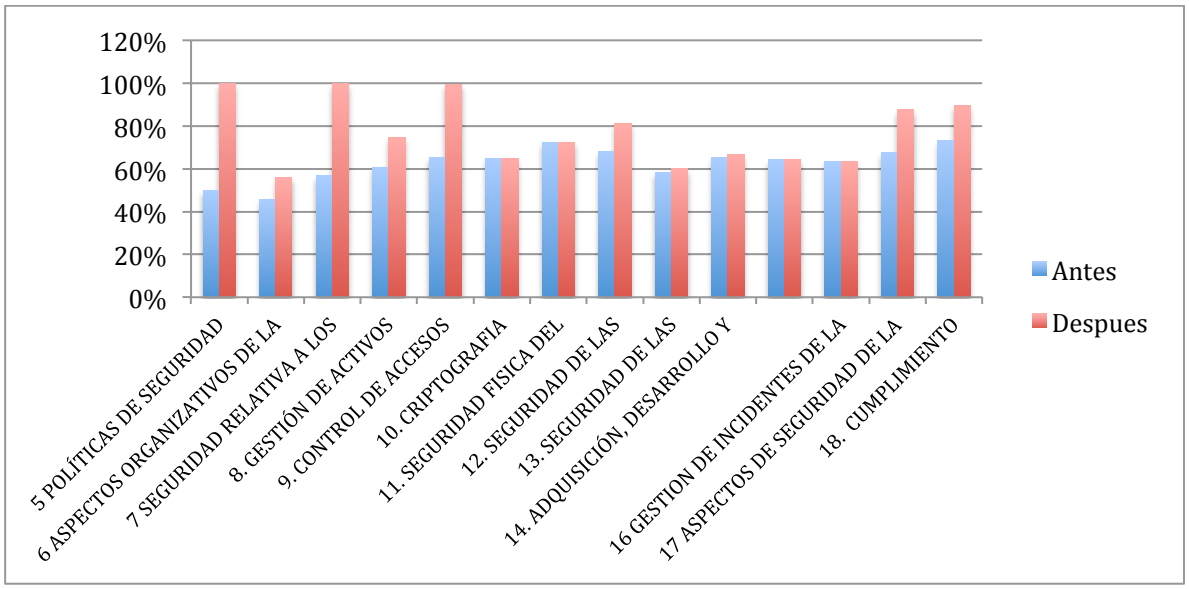
Dominio	Antes	Después
5 POLÍTICAS DE SEGURIDAD	50%	100%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	46%	56%
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	57%	100%
8. GESTIÓN DE ACTIVOS	61%	75%
9. CONTROL DE ACCESOS	65%	100%
10. CRIPTOGRAFIA	65%	65%
11. SEGURIDAD FISICA DEL ENTORNO	72%	72%
12. SEGURIDAD DE LAS OPERACIONES	68%	81%
13. SEGURIDAD DE LAS COMUNICACIONES	58%	60%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI	65%	66%
15. RELACIONES CON PROVEEDORES	64%	64%
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION	64%	64%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	68%	88%
18. CUMPLIMIENTO	73%	90%
CUMPLIMIENTO GENERAL	**63%**	**77%**

Dentro del modelo CMM el nivel general de cumplimiento de los diferentes controles antes de la implementación es Repetible. El nivel de cumplimiento general después de la implementación de los proyectos propuestos sube al nivel de Definido y para ciertos dominios específicos se puede tener niveles de cumplimiento optimizados. El porcentaje de cumplimiento después de la implementación de los proyectos sube de 63% a 77%.

El detalle del impacto de los proyectos planteados en los diferentes dominios de la norma ISO/IEC27002:2013 se puede encontrar en el ANEXO XIV.

En los siguientes gráficos se puede ver la evolución de los dominios de la norma ISO/IEC27002:2013 con respecto al cumplimiento antes y después de la realización de los proyectos.





5.5 Evolución de los Riesgos después de la implantación de los proyectos

Los proyectos propuestos buscan minimizar los niveles de riesgo para los activos mas críticos identificados durante la fase de análisis de riesgos.

Las valoraciones de la influencia de las amenazas sobre los activos, tanto en la degradación como en la probabilidad sufren modificaciones y disminuyen como consecuencia de la implementación de los proyectos.

Los controles que implementan los proyectos resultan ser reductores de la frecuencia de ocurrencia de amenazas en algunos casos, así como reductores del impacto de la amenaza en otros.

La siguiente tabla muestra el impacto que tienen los proyectos propuestos a través de los controles que aplican ya sea en la reducción de la frecuencia de ocurrencia de las amenazas y/o en el impacto de la materialización de la amenaza.

Reduce	Proyecto
Impacto	Políticas de seguridad de la Información
Frecuencia	Plan de Formación y concientización
Impacto/Frecuencia	Políticas de control de acceso y de acceso a la red y los servicios de red
Impacto/frecuencia	Gestión del acceso del usuario
Impacto	Plan de continuidad del Negocio
Impacto/frecuencia	Control de acceso al sistema y aplicaciones
Impacto	Revisión del SGSI
Frecuencia/impacto	Mejora en la gestión de Recursos Humanos
Frecuencia	2F autenticación
Frecuencia	Clasificación de la Información
Impacto	Copias de Respaldo

La tabla siguiente detalla la lista de amenazas cuya frecuencia de ocurrencia y/o impacto de ocurrencia son afectadas.

Amenazas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización
[E.7] Deficiencias en la organización
[E.15] Alteración accidental de la información

[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (SW)
[E.28] Indisponibilidad del personal
[A.4]Manipulación de la configuración
[A.5]Suplantación de la identidad del usuario
[A.6]Abuso de privilegios de acceso
[A.7]Uso no previsto
[A.8]Difusión de software dañino
[A.11]Acceso no autorizado
[A.15]Modificación deliberada de la información
[A.18]Destrucción de información
[A.19]Divulgación de información

El ANEXO XV lista la tabla de análisis de amenazas/activos después de la implementación de los proyectos. Esta tabla tiene los valores de frecuencia de ocurrencia y los valores de los impactos actualizados.

La siguiente tabla resume los impactos máximos de las diferentes amenazas para las 5 dimensiones de seguridad de los activos.

Activo	Impacto				
	A	C	I	D	T
[D] Datos- Información	75%	75%	75%	75%	75%
[S] Servicios	50%	50%	50%	50%	75%
[SW] Software	50%	75%	50%	100%	
[HW] Hardware		100%	20%	100%	
[AUX] Equipo Auxiliar		50%	75%	100%	
[COM]: Redes		100%	20%	100%	
[I] Instalaciones		20%	5%	100%	
[P] Personal		50%	20%	100%	

Con los nuevos valores de frecuencia y valores de impactos calculamos el impacto potencial y luego el riesgo después de la implementación de los proyectos.

El calculo del riesgo residual se encuentra en el ANEXO XVI.

Como se puede observar de los resultados de este calculo, los riesgos residuales bajan de niveles.

Estos resultados muestran que los proyectos que se han implementado han

cumplido el objetivo de mitigar los riesgos y tratar con prioridad los riesgos prioritarios que fueron definidos siendo estos los críticos.

Sin embargo como se muestra en las tablas a continuación existen riesgos que sin ser críticos se encuentran por encima del umbral aceptable de la empresa por lo que es necesario que el proceso de mitigación de riesgos continúe.

A continuación se muestran las tablas resumen de los activos con el nivel de riesgo después de haber implementado los proyectos.

No existen riesgos críticos pero siguen existiendo riesgos altos.

	Activo	**Riesgo**
[SW.1]	Aplicación de gestión de datos clientes	ALTO
[SW.2]	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones	
[SW.3]	Aplicación de gestión de los datos personales de los empleados de la empresa	
[SW.4]	Aplicación de gestión de contratos de los clientes individuales	
[SW.5]	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas	
[SW.6]	Aplicación de gestión de contratos empresariales – seguros de grupo	
[SW.7]	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos	
[SW.8]	Aplicación contable de la empresa	
[SW.11]	Servidor de documentos en INT	
[SW.12]	Servidor de documentos en PRD	
[SW.16]	Servidor de aplicaciones de producción	
[SW.20]	SGBD Oracle en producción	
[HW.1]	Servidor de aplicaciones internas/finanzas/admini/compta	
[HW.2]	Servidores DNS	
[HW.3]	Servidores DB Oracle prod	
[HW.6]	Servidores DB Oracle int	
[HW.8]	Routers	
[HW.9]	Servidores de correo	
[HW.12]	Servidores de Integración	
[HW.13]	Servidores de Producción	
[HW.14]	PC Portables	
[HW.19]	Dispositivos de conexión VPN	
[HW.20]	Rack de comunicaciones	
[HW.21]	Switchs	
[HW.23]	Sistema Wifi	
[HW.24]	Cableado de la red	
[HW.26]	Servidor de documentos	

[HW.27]	Servidor de copias de seguridad	
[D.1]	Código fuentes aplicaciones de gestión de contratos	
[D.2]	Código fuente aplicaciones de gestión de usuarios	
[D.3]	Código fuente aplicaciones de gestión de datos de empleados	
[D.4]	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones	
[D.5]	Datos de clientes individuales	
[D.6]	Datos de clientes empresariales	
[D.7]	Datos de clientes independientes	
[D.8]	Datos de los empleados de la empresa	
[D.14]	Log de servidores y log de clientes	
[COM.1]	Internet	
[COM.2]	Red inalámbrica	
[COM.4]	Cableado telecomunicaciones	
[COM.6]	Red Local	
[COM.7]	Cableado eléctrico	
[S.1]	Servicio Web	
[S.3]	Servicios de archivos	
[S.4]	Servicios de documentos	
[S.7]	Servicio comunicaciones	
[S.9]	Portal Externo	
[AUX.7]	Cableado eléctrico	
[P.1]	Director General	
[P.2]	Director IT	
[P.3]	Director operaciones	
[P.8]	Gestionaros de contratos/Business Experto	
[P.10]	Administrador de la aplicación	

	Activo	Riesgo
[SW.9]	Servidor de documentos de desarrollo	
[SW.10]	Servidor de documentos en TST	
[SW.13]	Servidor de aplicaciones de desarrollo	
[SW.14]	Servidor de aplicaciones de test	
[SW.15]	Servidor de aplicaciones de integración	
[SW.17]	SGBD Oracle en desarrollo	
[SW.18]	SGBD Oracle en test	MEDIO
[SW.19]	SGBD Oracle en integración	
[HW.4]	Servidores DB Oracle dev	
[HW.5]	Servidores DB Oracle test	
[HW.7]	Servidores de e-comerce	
[HW.10]	Servidores de Desarrollo	
[HW.11]	Servidores de Test	

[HW.15]	PC de escritorio fijas	
[HW.16]	Tabletas	
[HW.22]	Firewalls	
[HW.25]	Cámaras de vigilancia	
[HW.28]	Multiservidores de impresión/scanner/fotocopias	
[D.9]	Datos de acceso a las aplicaciones (roles y responsabilidades)	
[D.10]	Documentos de clientes	
[D.11]	Documentos de empleados	
[D.12]	Documentos otros	
[D.13]	Datos de soporte y licencias	
[D.15]	Backup de DB users	
[D.16]	Documentos en papel (contratos)	
[D.17]	Backup código fuente	
[D.18]	Backuo de DB Clientes	
[D.19]	Backup DB empleados	
[D.20]	Datos de configuración	
[COM.3]	RED telefónica	
[COM.5]	Telefonía móvil	
[S.2]	Servicio de aplicaciones	
[S.5]	Servicios DNS	
[S.6]	Servicios email	
[S.8]	Portal interno	
[AUX.1]	Lockers	
[AUX.2]	Multiprinters	
[AUX.8]	Mobiliario	
[P.5]	Director Finanzas	
[P.7]	Personal de desarrollo de las aplicaciones	
[P.11]	Técnicos de soporte buSiness	
[P.12]	Agentes de ventas	
[P.13]	Personal Comercial	
[P.14]	Personal Finanzas	
[P.15]	Personal Infraestructura	
[P.16]	Personal Risks	
[P.17]	Administradores de sistemas	
[P.18]	Personal de soporte IT	

	Activo	Riesgo
[HW.17]	Teléfonos fijos	
[HW.18]	Teléfonos móviles	
[AUX.3]	Recursos varios (material de escritorio, maletas, …)	
[AUX.4]	Televisores	

[AUX.5]	Equipos de sonido y proyección	BAJO
[AUX.6]	Pantallas	
[P.4]	Director de recursos humanos	
[P.4]	Directos Riesgos	
[P.9]	Personal RH	
[P.6]	Director Marketing y ventas	

	Activo	Riesgo
[I.1]	Centro de procesamiento de datos	MUY BAJO
[I.2]	Salas de Reuniones	
[I.3]	Puestos de trabajo del personal – open spaces	
[I.4]	Puestos de trabajo bajo seguro	
[I.5]	Oficinas de los directivos	
[I.6]	Salas de impresión	
[I.7]	Unidades de apoyo a los servicios	
[I.8]	Espacios de almacenamiento de los racks	
[I.9]	Espacio de almacenamiento de documentos papel seguros	

6. Fase 5: Auditoria de cumplimiento

6.1 Introducción

En esta fase se evalúa hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 sirve como marco de control del estado de la seguridad. Se busca comprobar el nivel de madurez de la seguridad en la empresa.

A continuación se documentarán las diferentes fases del proceso de auditoría de cumplimiento y una vez comprobada la madurez de los controles ISO / IEC 27002: 2013 se informará de las no conformidades encontradas por tanto de solucionarlas y poder obtener la certificación de la norma sin problemas.

Para finalizar la auditoría de cumplimiento veremos los resultados obtenidos comparándolos con el estado de madurez de los controles al inicio del proyecto.

6.2 Metodología

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control.

Hay diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo, ya hablemos de los controles ISO/IEC 27002:2013 o de cualquier otro catálogo. Estos son en general:

1. Formalización de las prácticas mediante documentos escritos o aprobados.
2. Política de personal.
3. Solicitudes técnicas (software, hardware o comunicaciones).
4. Seguridad física.

La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

6.3 Evaluación de la madurez

La evaluación de la madurez de la seguridad se la realiza con respecto a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Los dominios a analizar son los siguientes:

Dominios
5 POLÍTICAS DE SEGURIDAD
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS
8. GESTIÓN DE ACTIVOS

9. CONTROL DE ACCESOS
10. CRIPTOGRAFIA
11. SEGURIDAD FISICA DEL ENTORNO
12. SEGURIDAD DE LAS OPERACIONES
13. SEGURIDAD DE LAS COMUNICACIONES
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI
15. RELACIONES CON PROVEEDORES
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS
18. CUMPLIMIENTO

Este estudio realiza una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control. Esta estimación se la realiza según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. 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. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. 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. 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. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Se evalúa uno a uno los diferentes controles para cada uno de los dominios y se verifica la conformidad de los controles.

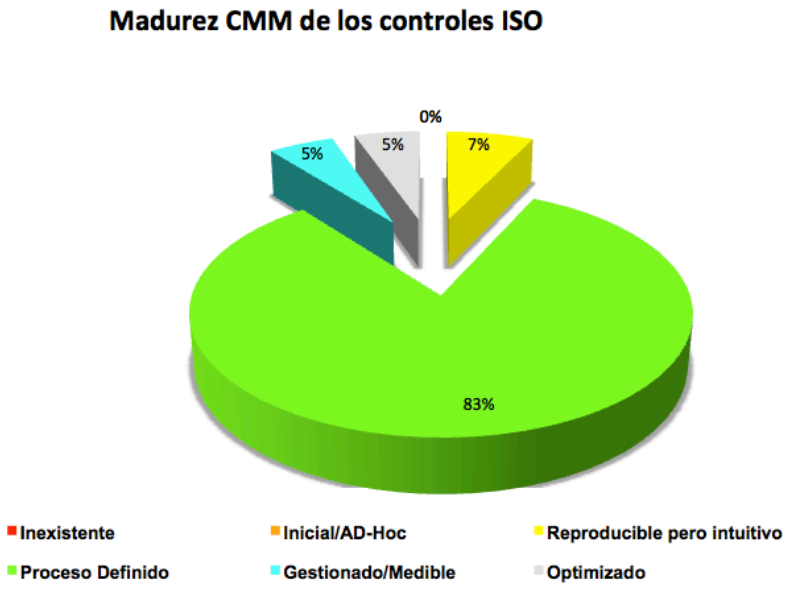
El ANEXO XVII se muestra el detalle de esta evaluación del cumplimiento de la norma.

6.4 Presentación de resultados

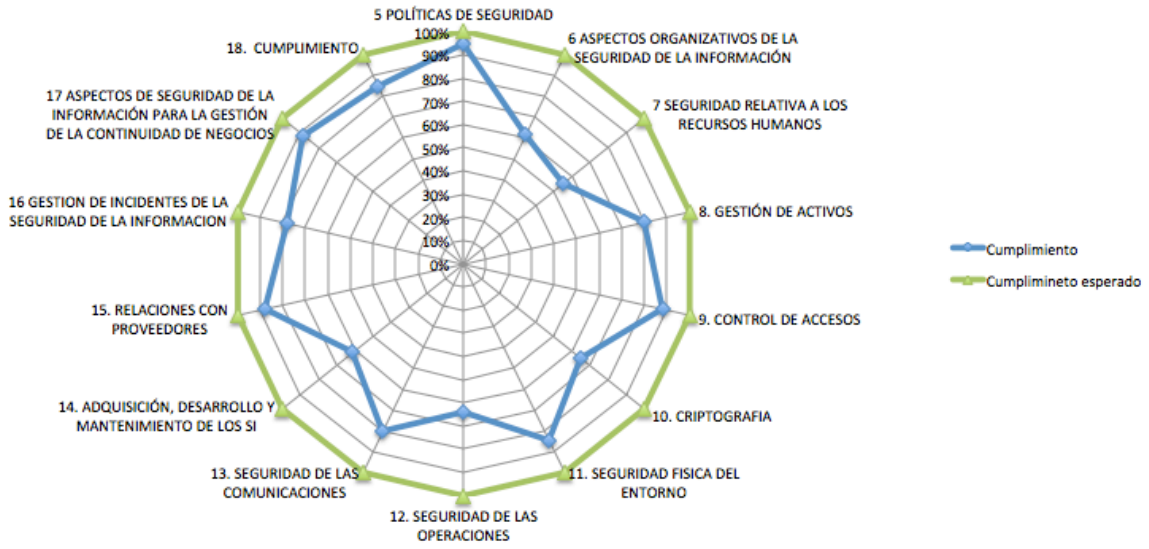
De los resultados de la evaluación la siguiente tabla resume el número de controles implementados que se encuentran dentro de los niveles de madurez especificados.

Nivel de Madurez	No Controles
Inexistente	0
Inicial/AD-Hoc	0
Reproducible pero intuitivo	8
Proceso Definido	94
Gestionado/Medible	6
Optimizado	6
Total	114

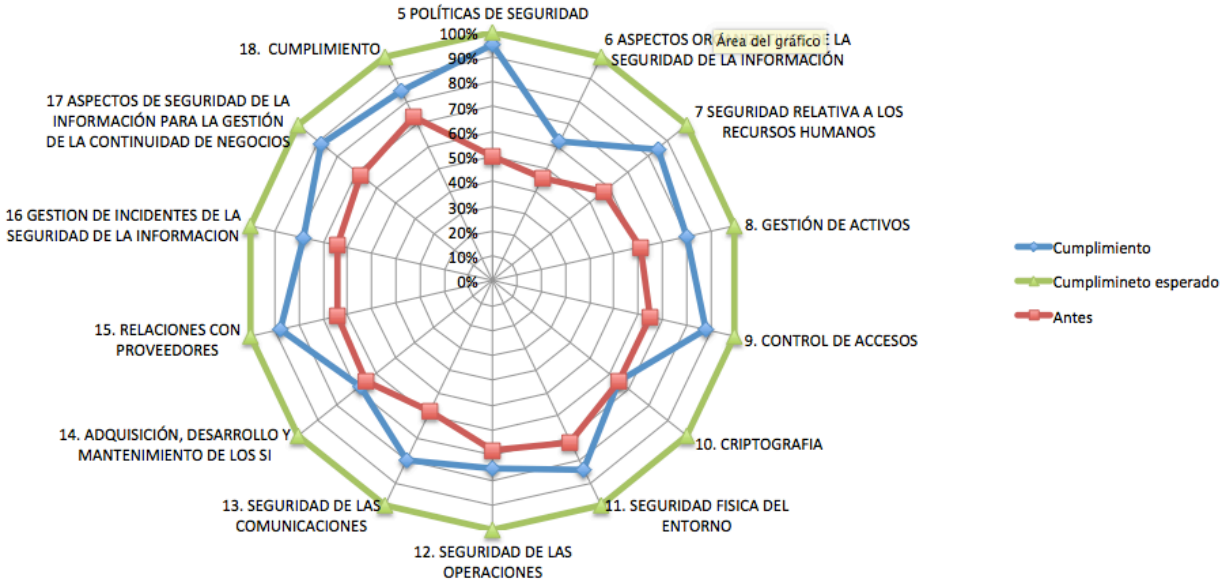
En la siguiente grafica podemos observar el nivel de madurez porcentual de los controles implementados para cada uno de los niveles de madurez CMM.



Una visión detallada es la que se presenta como 'diagrama de radar' que muestra el nivel de cumplimiento para cada unos de los dominios. Los niveles de cumplimiento se expresan en función de los porcentajes calculados para cada unos de los dominios.

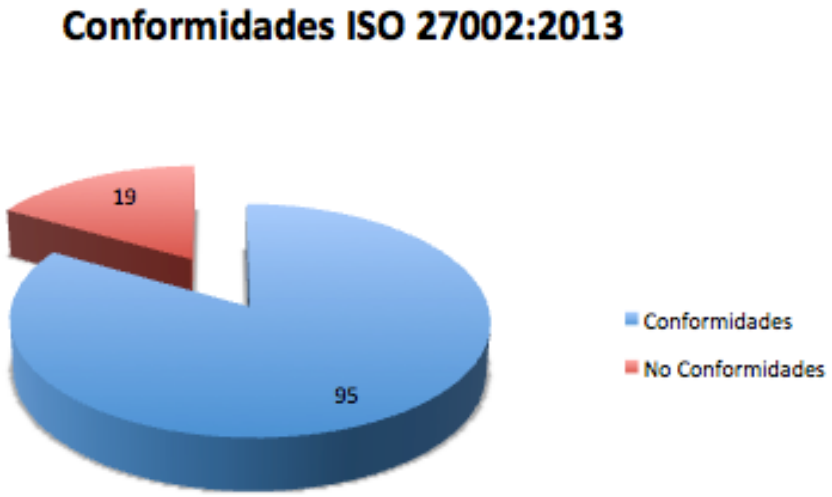


En el siguiente grafico podemos ver que existe una mejora general en el nivel de cumplimiento de los diferentes dominios de la norma comparados con el análisis diferencial realizado al inicio del proyecto.



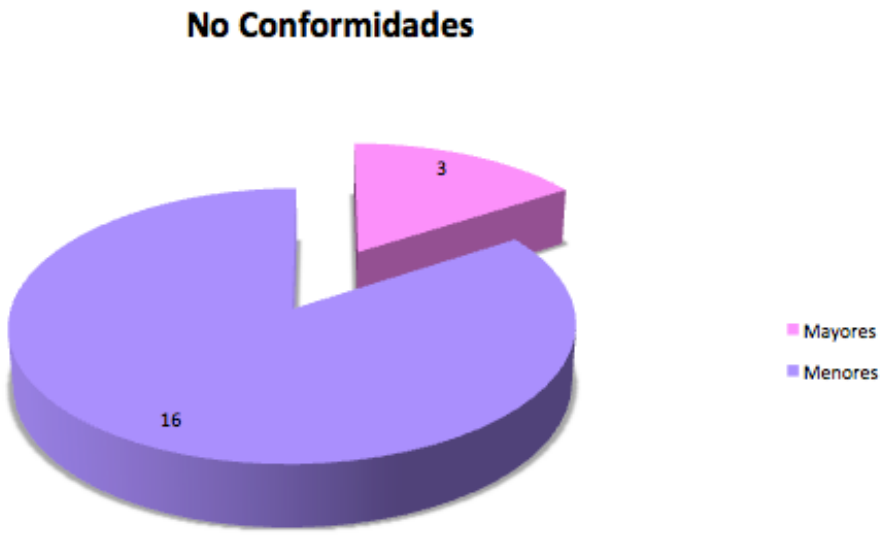
Del resultado de la evaluación de los 114 controles de la norma, se han identificado 19 controles que no cumplen con lo que especifica la norma.

En el siguiente grafico se muestra la relación entre las conformidades y las no conformidades con respecto a la norma.



La siguiente tabla resume para los diferentes dominios de la norma el numero de controles que no cumplen. Se han identificando las no conformidades mayores y menores.

Dominios	Mayores	Menores
5 POLÍTICAS DE SEGURIDAD		
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		3
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS		
8. GESTIÓN DE ACTIVOS		
9. CONTROL DE ACCESOS	3	
10. CRIPTOGRAFIA		1
11. SEGURIDAD FISICA DEL ENTORNO		2
12. SEGURIDAD DE LAS OPERACIONES		4
13. SEGURIDAD DE LAS COMUNICACIONES		
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI		4
15. RELACIONES CON PROVEEDORES		
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION		1
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS		
18. CUMPLIMIENTO		1
	3	16



La lista de inconformidades se encuentra detallada en el informe de auditoria disponible en el ANEXO XVIII.

6.3 Conclusiones

Una vez completada esta fase, tenemos una visión del cumplimiento de los diferentes dominios de la ISO/IEC 27002:2013 y de su incumplimiento.

Los resultados confirman que la empresa está trabajando en la implementación de los controles necesarios con miras a garantizar un manejo seguro de la información. Si bien es cierto que no se ha llegado al nivel optimizado. De los resultados muestran que la empresa es consiente de la importancia de la seguridad de la información y por ello trabaja en la implementación de los diferentes dominios con miras a alcanzar niveles de madurez cada vez superiores.

7. CONCLUSIONES

La implementación de un Plan de Seguridad de la Información es un proceso continuo que busca mejorar de los niveles de Seguridad en el manejo de la Información.

Se ha comprobado que la implementación de este plan ha mejorado el nivel de seguridad de la información en la empresa.

El éxito de este requiere de la participación y del compromiso de todos los miembros del personal. Encabezados por una Dirección comprometida con el proceso se ha logrado definir y aprobar un conjunto de políticas y procedimientos para un manejo seguro de la información dentro de la organización.

De igual manera se ha creado una estructura interna con responsabilidad directa sobre la seguridad de la información. Se han definido los roles y las responsabilidades.

Este plan constituye la única guía corporativa que implementa de las medidas de seguridad de la información y los sistemas de información dentro de la organización.

El plan de formación/concientización es fundamental para la evolución exitosa de este plan. Si bien se ha logrado mejorar los niveles de concientización del personal, se recomienda que el proceso de formación sea continuo.

Se puede concluir que se ha creado una cultura de seguridad dentro de la empresa.

ANEXOS

ANEXO I

Tablas Análisis Diferencial

La siguiente tabla muestra el resultado del análisis diferencial de las medidas de seguridad que la empresa A2 tiene actualmente implantadas respecto los requisitos que conforman la norma ISO 27002:2013.

No	Requisitos	Estado
4	Contexto de la organización	55%
4.1	Comprender la organización en su contexto	50%
4.2	Comprender las necesidades y expectativas de las partes interesadas	70%
4.3	Determinar el alcance del SGSI	50%
4.4	SGSI	50%
5	Liderazgo	43%
5.1	Liderazgo y compromiso	30%
5.2	Política	50%
5.3	Roles organizacionales, responsabilidades y autoridades=	50%
6	Planificación	50%
6.1	Acciones para abordar los riesgos y las oportunidades	50%
6.2	Objetivos de la seguridad de la información	50%
7	Apoyo	58%
7.1	Recursos	70%
7.2	Competencias	50%
7.3	Conocimiento	70%
7.4	Comunicación	50%
7.5	Información documentada	50%
8	Operación	50%
8.1	Control y planificación operacional	50%
8.2	Evaluación de riesgo de la SI	50%
8.3	Tratamiento del riesgo de la SI	50%
9	Evaluación de desempeño	43%
9.1	Monitoreo, medición, análisis y evaluación	50%
9.2	Auditoria interna	30%
9.3	Revisión de gestión	50%
10	Mejora	50%
10.1	No conformidades y acciones correctivas	50%
10.2	Mejora continua	50%

La siguiente tabla muestra el resultado del análisis diferencial de las medidas de seguridad que la empresa A2 tiene actualmente implantadas con respecto a los controles que conforman la norma ISO 27001:2013.

Control	Cumplimiento
5 POLÍTICAS DE SEGURIDAD	50%
5.1 Directrices de la Dirección en seguridad de la información	50%
5.1.1 Conjunto de políticas para la seguridad de la información	60%
5.1.2 Revisión de las políticas para la seguridad de la información	40%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	46%
6.1 Organización interna	49%
6.1.1 Asignación de responsabilidades para la seguridad de la información	60%
6.1.2 Segregación de tareas	60%
6.1.3 Contacto con las autoridades	70%
6.1.4 Contacto con grupos de interés especial	70%
6.1.5 Seguridad de la información en la gestión de proyectos	30%
6.2 Dispositivos para movilidad y teletrabajo	43%
6.2.1 Política de uso de dispositivos para movilidad	40%
6.2.2 Teletrabajo	45%
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	57%
7.1 Antes de la contratación	60%
7.1.1 Investigación de antecedentes	60%
7.1.2 Términos y condiciones de contratación	60%
7.2 Durante la contratación	60%
7.2.1 Responsabilidades de gestión	60%
7.2.2 Concienciación, educación y capacitación en seguridad de la información	60%
7.2.3 Proceso disciplinario	60%
7.3 Cese o cambio de puesto de trabajo	50%
7.3.1 Cese o cambio de puesto de trabajo	50%
8. GESTIÓN DE ACTIVOS	61%
8.1 Responsabilidad sobre los activos	70%
8.1.1 Inventario de activos	80%
8.1.2 Propiedad de los activos	70%
8.1.3 Uso aceptable de los activos	60%
8.1.4 Devolución de activos	70%
8.2 Clasificación de la información	70%
8.2.1 Directrices de clasificación	70%
8.2.2 Etiquetado y manipulado de la información	70%
8.2.3 Manipulación de activos	70%

8.3 Manejo de los soportes de almacenamiento	42%
8.3.1 Gestión de soportes extraíbles	40%
8.3.2 Eliminación de soportes	45%
8.3.3 Soportes físicos en tránsito	40%
9. CONTROL DE ACCESOS	65%
9.1 Requisitos de negocio para el control de accesos	70%
9.1.1 Política de control de accesos	80%
9.1.2 Control de acceso a las redes y servicios asociados	60%
9.2 Gestión de acceso de usuario	58%
9.2.1 Registro de acceso y baja de usuarios	70%
9.2.2 Provisión de acceso de usuario	60%
9.2.3 Gestión de privilegios de acceso	60%
9.2.4 Gestión de la información secreta de autenticación de los usuarios	50%
9.2.5 Revisión de los derechos de acceso del usuario	55%
9.2.6 Retirada o reasignación de los derechos de acceso	55%
9.3 Responsabilidades del usuario	65%
9.3.1 Uso de la información secreta de la autenticación	65%
9.4 Control de acceso a sistemas y aplicaciones	68%
9.4.1 Restricción de acceso a la información	80%
9.4.2 Procedimientos seguros de inicio de sesión	60%
9.4.3 Sistema de gestión de contraseñas	70%
9.4.4 Uso de utilidades con privilegios del sistema	70%
9.4.5 Control de acceso al código fuente de los programas	60%
10. CRIPTOGRAFIA	65%
10.1 Controles criptográficos	65%
10.1.1 Política de uso de los controles criptográficos	60%
10.1.2 Gestión de claves	70%
11. SEGURIDAD FISICA DEL ENTORNO	72%
11.1 Áreas seguras	78%
11.1.1 Perímetro de seguridad física	80%
11.1.2 Controles físicos de entrada	90%
11.1.3 Seguridad de oficinas, despachos y recursos	70%
11.1.4 Protección contra las amenazas externas y ambientales	80%
11.1.5 El trabajo en áreas seguras	80%
11.1.6 Áreas de carga y descarga	70%
11.2 Seguridad de los equipos	66%
11.2.1 Emplazamiento y protección de equipos	65%
11.2.2 Instalaciones de suministro	80%
11.2.3 Seguridad del cableado	80%
11.2.4 Mantenimiento de los equipos	80%
11.2.5 Retirada de materiales propiedad de la empresa	60%
11.2.6 Seguridad de los equipos fuera de las instalaciones	60%

11.2.7 Reutilización o eliminación segura de equipos	60%
11.2.8 Equipo de usuario desatendido	60%
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	50%
12. SEGURIDAD DE LAS OPERACIONES	68%
12.1 Procedimientos y responsabilidades operacionales	55%
12.1.1 Documentación de procedimientos de las operaciones	70%
12.1.2 Gestión de cambios	50%
12.1.3 Gestión de capacidades	50%
12.1.4 Separación de los recursos de desarrollo, prueba y operaciones	50%
12.2 Protección contra el software malicioso	70%
12.2.1 Controles contra el código malicioso	70%
12.3 Copias de seguridad	70%
12.3.1 Copias de seguridad de la información	70%
12.4 Registros y supervisión	63%
12.4.1 Registro de eventos	70%
12.4.2 Protección de la información de registro	60%
12.4.3 Registros de administración y operación	70%
12.4.4 Sincronización del reloj	50%
12.5 Control del software en explotación	60%
12.5.1 Instalación del software en explotación	60%
12.6 Gestión de la vulnerabilidad técnica	50%
12.6.1 Gestión de la vulnerabilidad técnica	50%
12.6.2 Restricción en la instalación del software	50%
12.7 Consideraciones sobre la auditoria de sistemas de información	40%
12.7.1 Controles de auditoria de sistemas de información	40%
13. Seguridad de las comunicaciones	58%
13.1 Gestión de la seguridad de redes	47%
13.1.1 Controles de red	50%
13.1.2 Seguridad de los servicios de red	50%
13.1.3 Segregación en redes	40%
13.2 Intercambio de información	70%
13.2.1 Políticas y procedimientos en intercambio de información	60%
13.2.2 Acuerdos de intercambio de información	70%
13.2.3 Mensajería electrónica	70%
13.2.4 Acuerdos de confidencialidad o no revelación	80%
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	65%
14.1 Requisitos de seguridad en sistemas de información	70%
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	60%
14.1.2 Asegurar los servicios de aplicaciones en redes publicas	70%

14.1.3 Protecciones de las transacciones de servicios de aplicaciones	80%
14.2 Seguridad en el desarrollo y en los procesos de soporte	56%
14.2.1 Política de desarrollo seguro	50%
14.2.2 Procedimiento de control de cambios en el sistema	50%
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	70%
14.2.4 Restricciones a los cambios en los paquetes de software	50%
14.2.5 Principios de ingeniería de sistemas seguros	50%
14.2.6 Entorno de desarrollo seguro	50%
14.2.7 Externalización del desarrollo de software	50%
14.2.8 Pruebas funcionales de seguridad del sistema	70%
14.2.9 pruebas de aceptación del sistema	65%
14.3 Datos de prueba	70%
14.3.1 Protección de los datos de prueba	70%
15. RELACIONES CON PROVEEDORES	64%
15.1 Seguridad en las relaciones con los proveedores	73%
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	70%
15.1.2 Requisitos de seguridad en contratos con terceros	75%
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	75%
15.2 gestión de la provisión de los servicios del proveedor	55%
15.2.1 Control y revisión de la provisión de servicios del proveedor	55%
15.2.2 Gestión de cambios en la provisiones del proveedor	55%
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION	64%
16.1 Gestión de incidentes de seguridad de la información y mejoras	64%
16.1.1 Responsabilidades y procedimientos	60%
16.1.2 Notificación de los eventos de seguridad de la información	60%
16.1.3 Notificación de puntos débiles de la seguridad	60%
16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	65%
16.1.5 Respuesta a incidentes de seguridad de la información	75%
16.1.6 Aprendizaje de los incidentes de seguridad de la información	60%
16.1.7 Recopilación de evidencias	65%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	68%
17.1 Continuidad de la seguridad de la información	60%
17.1.1 Planificación de la continuidad de la seguridad de la información	60%
17.1.2 Implementar la continuidad de la seguridad de la información	60%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	60%
17.2 Redundancias	75%
17.2.1 Disponibilidad de los recursos de tratamientos de la información	75%

18. CUMPLIMIENTO	73%
18.1 Cumplimiento de los requisitos legales y contractuales	73%
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	80%
18.1.2 Derechos de propiedad intelectual	80%
18.1.3 Protección de los registros de la organización	80%
18.1.4 Protección y privacidad de la información de carácter personal	70%
18.1.5 Regulación de los controles criptográficos	55%
18.2 Revisiones de la seguridad de la información	73%
18.2.1 Revisiones independientes de la seguridad de la información	75%
18.2.2 Cumplimiento de las políticas y de las normas de seguridad	70%
18.2.3 Comprobación del cumplimiento técnico	75%

ANEXO II

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA A2

1. Objetivo

El objetivo de la presente política es establecer las directivas de base relacionadas con la seguridad de la información y que contribuyan a garantizar:

1. La confidencialidad de la información.
2. La integridad de la información.
3. La disponibilidad de la información

2. Alcance y aplicación de la seguridad

La Política de Seguridad de la información se aplicará en todas las áreas de la empresa como una política básica, siempre que la aplicación de una política u otra sea relevante para cada caso.

3. Principios de seguridad

La política de seguridad de A2 incluye una serie de principios de seguridad. Estos principios incluyen las siguientes áreas:

1. Protección de la información
2. Controles de acceso Sistemas
3. Los privilegios de acceso
4. El acceso remoto
5. Controles basados en el riesgo del negocios
6. Clasificación de la información
7. Propiedad de la información
8. Gestión de las excepciones de seguridad
9. Políticas ejecutables y prácticas
10. Cumplimiento de las obligaciones reglamentarias y legales
11. Estándares reconocidos
12. Informar a los usuarios de la política

Estos principios has sido creados para determinar la criticidad de los sistemas y los niveles de protección necesarios y así satisfacer los requerimientos legales.

4. El activo de la información, clasificación y responsabilidad.

a. Activos de Información e Inventario

Todos los principales activos de información deben ser contabilizados y deben tener un propietario designado. Elaborar un inventario sobre los activos de información asociados a cada uno de los sistemas de TI. Se elabora un inventario de los principales activos de información asociados a los sistema

de TI. Cada activo será documentado con los detalles del sistema IT asociado, del propietario, y su clasificación en materia de seguridad.

b. Clasificación de la información

La empresa posee una matriz de clasificación de la información que es utilizada como guía para este proceso.
Toda información de la empresa debe ser identificada, clasificada y documentada de acuerdo a la guía de clasificación establecida por el comité de seguridad.
Una vez clasificada la información se otorgaran los recursos necesarios para la aplicación de controles con miras a garantizar la confidencialidad, integridad y disponibilidad de la misma.

c. Asignación de Responsabilidades de Seguridad de Información

El propietario de un activo puede delegar sus responsabilidades de seguridad a otros, pero este sigue siendo el responsable ultimo de su protección. El delegado compartirá la responsabilidad de la información bajo su cargo.

d. Análisis de riesgos

Cuando un análisis de riesgos ha sido realizado, procedimientos apropiados se deben poner en marcha para minimizar el riesgo al que esta expuesto.

e. Seguridad de Acceso de Terceros
El acceso de terceros a instalaciones y servicios de la Empresa A2 no es posible a menos que hayan sido implementadas medidas adecuadas de seguridad y un contrato definiendo los términos de conexión haya sido firmado. Los terceros son generalmente las entidades comerciales u organizaciones que dan o reciben servicios de la empresa.

Otras como las relaciones con las instituciones de gobierno, entidades regulatorias y socios comerciales se reconocen, para efectos de estas normas, como afiliados de la empresa, y cuentan con acceso a determinados Sistemas Informáticos manejados por la empresa.
Los contratos relacionados con terceros IT deben incluir SLA's que cubran específicamente cómo las terceras partes gestionaran la información.

Para cubrir las situaciones en las que los usuarios de las terceras partes se encuentran en incumplimiento de la Política de Seguridad, los contratos deben incluir cláusulas estándares permitiendo que la empresa A2 pueda cancelar dichos contratos sin penalización. Esto sólo se ejercerá en situaciones de violaciones graves de la política

5. Sistemas de información y control de acceso

a. Políticas de acceso y procedimientos

El acceso a los servicios informáticos de gestión de la empresa A2 y el procesamiento de la información sensible será controlado mediante un acceso restringido sólo a usuarios autorizados.

Cada proveedor de servicios al interior de la empresa debe mantener una declaración de política de acceso de usuario definido que debe tomar en cuenta:

- Los requisitos de seguridad de los sistemas de información de unidad individuales
• Políticas y normas para la difusión de información y el derecho a la misma
• Los perfiles de seguridad deben ser establecidos para categorías de acceso común.
• El uso de privilegios especiales debe ser restringido y controlado. Esto debe ser visto como una asignación innecesaria y como un factor importante que contribuye en la vulnerabilidad de los sistemas.
• Deben existir procedimientos formales de registro y baja de usuarios.

El acceso a los servicios IT multiusuarios deben ser controlados a través de un proceso de registro formal que debe:

- verificar que el usuario tiene la autorización del dueño del sistema para utilizar el servicio.
- Verificar que el nivel de acceso es apropiado
- Dar a los usuarios una declaración escrita de sus derechos de acceso y sus responsabilidades.
- exigir a los usuarios a firmar compromisos que confirman que han leído la política de Seguridad y que entienden las condiciones, los niveles y el tipo de acceso que se les ha asignado.
- Tener la certeza de que los acceso no son concedidos hasta que los procedimientos de registro han sido completados;
- Guardar un registro formal de todas las personas registradas a utilizar el servicio, la fecha y hora de caducidad.
- Asegurar que el acceso se elimina rápidamente al final del período.
- Controlar y eliminar periódicamente las cuentas caducadas y/o redundantes.

Siempre que sea posible no se debe promover la creación de las cuentas ‘guest’ o anónimas. Si es necesario este tipo de cuentas, estas tendrán accesos mínimos y su utilización debe ser estrictamente controladas.

En caso de que sea necesario el procesamiento de la información en los sistemas multiusuario de la empresa, se requiere:
- Identificación y verificación de la identidad de cada usuario autorizado por medio de un proceso de autenticación efectivo.
- Proporcionar un sistema de gestión de acceso que asegura una de códigos de autenticación de calidad.
- Cuando sea necesario, se harán restricciones del tiempo de conexión de los usuarios y la aplicación de los umbrales de tiempo de espera.

b. Procesos de autenticación seguros

La check-list siguiente debe formar parte integral de cualquier proceso seguro de inicio de sesión:

- Mostrar un aviso de advertencia que la computadores sólo debe ser accedida por usuarios autorizados.
- Limitar el numero de inicio de sesiones fallidas (se recomienda 3 o 4) antes de realizar alguna de :
    - Registrar el intento fallido.
    - Forzar un tiempo de retardo antes de permitir mas intentos de inicio de sesión.
    - Desconectas las conexiones de enlaces de datos
    - Desplegar la siguiente información cuando se realiza un inicio de sesión exitosa:
        - Fecha y hora del inicio de sesión precedente.
        - Detalles sobre intentos de inicio de sesión fallidos desde el último inicio de sesión exitosa.

c. Sistema de gestión de accesos

Se debe usar un sistema de gestión de acceso para autenticar los usuarios, y proporcionar controles para establecer estándares de códigos de autenticación, asegurando así que los usuarios tengan códigos de autenticación de calidad.
Un buen sistema de gestión de acceso debe:

- Forzar el uso de códigos de autenticación individuales para mantener la rendición de cuentas.
- Permitir a los usuarios elegir y cambiar sus códigos
- Forzar el numero mínimo de caracteres para el código (6-8 recomendado)
- Forzar el cambio de código a intervalos de tiempo predefinidos
- Forzar el cambio de códigos de autenticación temporales al primer inicio de sesión
- Tener un registro de códigos usados por el usuario e impedir la reutilización de códigos antiguos (6 meses).
- No desplegar nunca el código en la pantalla cuando este esta siendo escrito
- Almacenar los códigos de forma encriptado utilizando algoritmos one-way.
- Modificar los códigos por defecto después de las instalaciones de software
- Verificar que los códigos no se basan en las siguientes :
    - No sean fechas
    - Nombres de usuarios
    - Ids de usuarios
    - O otros sistemas de identificación
    - No mas de dos caracteres consecutivos o idénticos
    - Que no sean solo ni números ni letras

d. Control de acceso de los sistemas de información

Los sistemas de información deben tener controles de acceso lógicos para gestionar los accesos de la siguiente manera:

- Controlar el acceso de los usuarios y las funciones del sistema de acuerdo con la política de control de acceso definida
- Proporcionar protección contra accesos no autorizados para cualquier software que sea capaz de reemplazar/simular el sistema operativo o controles del sistema de información.
- Los controles de acceso no deben comprometer la seguridad de otros sistemas con los que se comparten recursos.

e. Monitoreo del acceso y uso del sistema

Los sistemas de información deben ser monitoreados para asegurar la conformidad con la política y los estándares de acceso.

Con el fin de disponer de herramientas eficaces de seguimiento y auditoría, es esencial e registro de todos los eventos susceptibles de ser dañinos, incluyendo excepciones, violaciones y otros eventos relevantes a la seguridad. Se debe hacer un seguimiento y registrarlos por un periodo de tiempo.

- Siempre que sea posible, los registros de eventos deben incluir los Ids de usuario, fechas y horas, direcciones o identificaciones de terminal.

Todos los relojes de sistema deben estar sincronizados de manera regular (mensualmente) para simplificar los rastreos entre diferentes sistemas.

6. Educación de los usuarios y responsabilidades

La Política de Seguridad de la Información de la empresa se pondrá a disposición y conocimiento de todos los usuarios autorizados.
Además se implementara un programa de capacitación adecuada para el uso correcto de las instalaciones IT y del software. Todos los usuarios deben estar conscientes de las amenazas y preocupaciones de la seguridad de la información y deben ser responsables de la implementación de la política de Seguridad Informática de la empresa.

a. Aceptación de responsabilidades por el usuario

Se debe exigir a los usuarios que firmen un compromiso que indique que han recibido, leído y aceptado respetar la política de seguridad. Los usuarios siempre deben tener en cuenta que la información y los recursos.

A los que se les ha concedido el acceso se deben utilizar únicamente para fines autorizados.
Los usuarios deben ser conscientes de que son responsables de las acciones realizadas bajo su identificador de usuario / contraseña y que serán considerados responsables bajo la ley si son negligentes en sus responsabilidades asociadas.

Dentro los sistemas sensibles de la empresa, los usuarios deben ser identificados y responsabilizados de forma individual. El acceso no debe ser compartido en ningún momento. Acciones disciplinarias son consideradas para cualquier usuario que infrinja esta política.

b. Autenticación

Los usuarios mantendrán confidenciales sus códigos de autenticación (contraseñas).
No existen cuentas de grupos de usuarios.
Cuando se crea por primera vez una cuenta de usuario, se debe proporcionar al usuario una código de autenticación (contraseña), que se ven obligados a cambiar de inmediato. Si un usuario olvida su contraseña, se le debe proporcionar de nuevo un código de autenticación temporal seguro, y que se vera obligado a cambiar de inmediato.
Los derechos de acceso de los usuarios deben revisarse periódicamente (max. 6 meses entre revisiones).
Los derechos de acceso a las cuentas privilegiadas deben revisarse con mayor frecuencia.

c. Equipos sin vigilancia

Todo equipo sin vigilancia debe tener implantada un sistema protección de seguridad apropiada.
Se deben incluir controles para ayudar con el bloqueo automático, el cierre automático de sesión o el time-out, controles de seguridad tales como cerraduras en los gabinetes de almacenamiento y salas de actividades.
Los usuarios son responsables de las infracciones realizadas en equipos sin vigilancia o desbloqueados.

Algunas buenas prácticas a adoptar:

- Terminar las sesiones activas una vez finalizadas las tareas, a menos que puedan ser protegidas por bloqueadores de pantallas.
- Cierre correcto de las sesiones en todos los equipos.
- Asegure el equipo de modo que se requiera un código de autenticación para volver a activarlo, o alguna otra clave física de bloqueo.

Cerrar con llave los ambientes donde reside la computadora si es apropiado.

d. Notificación de violaciones a la política

Los propietarios de la información deben establecer procedimientos para gestionar las infracciones de seguridad. Las infracciones se gestionarán de acuerdo con el nivel de riesgo generado, y puede incluir la presentación de informes a las instancias apropiadas.

Las infracciones por parte de los usuarios pueden enfrentar acciones disciplinarias.

Los contratos con terceros deben incluir clausuras para que los usuarios que violen la política de seguridad sean escoltados desde las instalaciones de la empresa y sus contratos cancelados sin penalizaciones para la empresa.

Todos los incidentes deben ser reportados a sus superiores directos.
Todo usuario con accesos mayores a los concedidos durante el proceso de su registro debe considerar esto como un incumplimiento de seguridad e informar inmediatamente.
Se debe informar todas las debilidades de seguridad observadas o presuntas en los sistemas o servicios.
Los usuarios no deben tratar de probar tales debilidades.
Los usuarios también deben informar del software que no cumplen según las especificaciones, ya sea a su unidad local de soporte de TI o al proveedor de servicio.

En todos los casos, el usuario debe:

- Hacer una nota escrita con los comandos, los síntomas y mensajes que aparezca en la pantalla.
- Dejar de usar la computadora y aislarla físicamente si es posible. Debe desconectarse de cualquier red (con la ayuda de un oficial de soporte informático) y encendida, a menos que se corra riesgo de que los archivos puedan ser alterados o borrados si la computadora se deja encendida.
- Informar inmediatamente a su responsable directo.

7. Seguridad física y ambiental para crítica y sensibilidad información

Los requisitos para la seguridad física variarán dependiendo de la escala y organización de los servicios IT y de la sensibilidad o importancia de la información y actividades que apoya.

Se debe considera la implementación de las siguientes medidas de seguridad:

a. Seguridad de las instalaciones

Las instalaciones IT que respalden las actividades críticas o delicadas se alojarán en zonas seguras con controles de entrada y barreras de seguridad. Deben estar protegidos físicamente de daños e interferencias.
Las barreras de seguridad deben reflejar el valor de los activos y los riesgos asociados.

El personal que suministra o mantiene servicios de apoyo sólo debe tener acceso cuando sea necesario y sea autorizado y, en su caso, su acceso debe ser restringido y sus actividades son controladas.
La selección y el diseño de los emplazamientos para albergar actividades críticas deben tener en cuenta los incendios, inundaciones y otros desastres naturales o provocados.

Los equipos de respaldo y los medios de copias de seguridad deben estar alojados fuera de la sede principal.

b. Política Clear Desk

Todas las unidades de trabajo deben adoptar la política de "Clear Desk Policy" para garantizar la confidencialidad de documentos sensibles, medios de almacenamiento y otros activos y poder reducir los riesgos de accesos no autorizados, robos o daños fuera de las horas de trabajo.

Cuando proceda se debe considerar:

- Los documentos sensibles y confidenciales, medios y otros activos deben ser guardados bajo llave cuando no son utilizados.
- La información sensible, laptops, PDAs, tabletas, y otros medios de valor deben estar guardados cunado no se los utiliza.
- Los computadores personales y terminales deben ser protegidas por candados, códigos de autenticación y otros controles cuando no son utilizados.
- Las licencias de software, CDs de instalación y manuales deben ser guardados con llave.

c. Eliminación de medios

La información sensible y confidencial de la empresa que se encuentra sobre cualquier forma de medio electrónico o no, no debe ser salir de la empresa sin la autorización adecuada del titular de la información o del propietario del sistema.
Se deben dar autorizaciones a los usuarios con acceso remoto para poder trabajar a distancia.

d. Directrices de Seguridad de los equipos

Los equipos deben estar físicamente protegidos de amenazas de seguridad y riesgos ambientales.
Es necesario proteger los equipos informáticos para reducir el riesgo de accesos no autorizados a los datos, y para protegerse contra pérdidas o daños.

Se puede utilizar la siguiente lista para identificar peligros potenciales:

- Fuego
- Humo
- Agua y otros líquidos.
- Polvo.
- Vibraciones.
- Efectos químicos.
- Interferencia del suministro eléctrico.
- Radiación electromagnética.
- Robo.

Fumar, comer y beber están prohibidas en las áreas de computación.

8. Ordenadores y gestión de redes

Los sistemas de la empresa serán mantenidos por personal debidamente capacitado.

a. Procedimientos operativos y responsabilidades

Se establecen responsabilidades y procedimientos para la gestión y el funcionamiento seguro de todas las computadoras y redes.
Esto incluye la provisión de un procedimiento de respuesta a incidentes.

b. Procedimientos de gestión de incidentes

Se establecen procedimientos de gestión de incidentes y responsabilidades para garantizar una gestión rápida, eficaz, una respuesta ordenada a los incidentes de seguridad.
Tal procedimiento variaría en alcance dependiendo de la sensibilidad y el tamaño de la información gestionada. Se establecerá un procedimiento de gestión de incidentes en toda la empresa, y se basará en la evaluación del riesgo tomando en cuenta:

- fallas del sistema y pérdidas de servicio;
- errores resultado de datos incompletos o inexactos; y
- violaciones de la confidencialidad.

Las acciones para corregir y recuperarse de las fallas de seguridad y del sistema deben esta formalmente controladas.
Los procedimientos deben asegurar que:

- Sólo el personal autorizado tiene acceso a los sistemas de información en línea y a los datos.
- Todas las medidas de emergencia tomadas están documentadas en detalle.
- Se notifica la acción de emergencia a la persona u órgano responsable y se revisa de forma ordenada.
- La integridad del sistema de información y los controles de seguridad se confirman en tiempos mínimos.

Los responsables de grande sistemas o sistemas con información sensibles debería considerar cubrir :

- el análisis e identificación de causas de incidentes
- planificación e implementación de remedios para prevenir la recurrencia
- recolección de pistas de auditoría y pruebas similares

Se deben recolectar y resguardar las pistas de auditoría y pruebas similares, según proceda para:
- Hacer un análisis de problemas internos;

- Utilizar como pruebas en relación con posibles incumplimientos de contrato o incumplimiento de los requisitos reglamentarios;
- Negociar compensaciones con proveedores de software y servicios

c. Protección contra software malintencionado

Todos los ordenadores y sistemas informáticos deben estar protegidos para prevenir / detectar la instalación de software malintencionado.

Se deben tomar precauciones para prevenir y detectar la instalación de software malicioso.

Los administradores de ordenadores y sistemas informáticos deben estar atentos a los peligros del software malicioso, y deben tomar medidas necesarias para prevenir o detectar la instalación de dicho software.

Es esencial que se tomen precauciones para prevenir y detectar las formas actualmente conocidas de software malintencionado y virus informáticos en ordenadores personales. Esto requiere de procesos probados y planificados para distribuir las actualizaciones para resolver vulnerabilidades identificadas del sistema.

d. Control de virus

Se deben implementar medidas de detección y prevención de virus y de procedimientos apropiados de sensibilización.
Los usuarios deben recordar que la prevención es mucho mejor que curar. La base de la protección contra los virus debe basarse en una buena conciencia de seguridad y un adecuado sistema de control de acceso.
Se debe establecer una política de licencias de software que prohíba el uso de software no autorizado.
El software antivirus a ser utilizado debe ser desarrollado por un proveedor de confianza y debe usarse de la siguiente manera:

- Utilizar software de detección de virus (que debe actualizarse periódicamente y utilizarse siguiendo las consignas del proveedor) para escanear computadoras y soportes de virus conocidos, como medida de precaución de forma rutinaria.
- Se debe instalar software de detección de cambios donde sea apropiado, para detectar cambios en el código ejecutable.
- El Software de "reparación" de virus debe utilizarse con precaución y sólo en los casos donde se tenga control pleno.
- Considerar la realización de revisiones periódicas del software y el contenido de datos de los procesos críticos. La presencia de archivos falsos o de enmiendas no autorizadas deben ser formalmente investigadas.
- Cualquier disco o CD de origen incierto o no autorizado debe ser revisado contra los virus.
- Deben establecerse procedimientos y gestión de responsabilidades para informar y recuperar los ataques de virus.

- Se deben establecer planes apropiados para la recuperación de datos y las copias de seguridad.

e. Controles de seguridad de red

Deben establecerse controles adecuados para garantizar la seguridad de los datos en las redes privadas y públicas, así como la protección de los servicios contra el acceso no autorizado. La infraestructura de la red debe estar protegida de accesos no autorizados.

Se requiere una serie de controles de seguridad en las redes de computadoras para proteger los entornos.
Los usuarios individuales deben ser conscientes de que conectar su computadora a la red puede permitir accesos no autorizado a datos privados si no se establecen controles adecuados.
La documentación debe estar disponible para el usuario detallando cómo asegurar adecuadamente sus datos si lo desean disponibles en una red.
Los gestores de las redes deben velar por que se establezcan controles adecuados para garantizar los datos en las redes y la protección de los servicios contra los accesos no autorizados.
Se debe prestar atención especial a la protección de información sensible que transita por las redes públicas.

Se debe disponer de herramientas que permiten monitorear los puertos de la red y/o el funcionamiento de la red al ser interrumpida.
Con el fin de minimizar el riesgo de interferencia en la red se debe prestar atención:

- Protección del cableado en áreas públicas con conductos u otros mecanismos de protección.
- En un área de cableado estructurado, asegurarse de que los puntos de red y de teléfono que no están en uso hayan sido desconectado de la red activa o del equipo de telefonía.
- Los redes de datos y de telefonía solo pueden ser accedidos por personal autorizados.
- La información que se transfiere a través de redes no seguras está encriptado.
- Los puntos de accesibilidad, como los módems en red deben estar asociados a mecanismos de seguridad.

9. Requisitos de seguridad de los sistemas de información

Un análisis de los requisitos de seguridad debe formar parte de cualquier propuesta para adquirir o mantener sistemas de información de la empresa y asegurar de esta manera que el sistema resultante cumpla con la Política de Seguridad.
La política de seguridad la información y estas normas requieren una revisión periódica de las medidas de seguridad implementadas en los sistemas de información de la empresa para mantener el cumplimiento de la seguridad.

Los requisitos de seguridad para los sistemas deben ser identificados y acordados como requisitos, antes del desarrollo.
Los requisitos y controles de seguridad deben reflejar el valor de la información involucrada para la empresa, y el daño potencial que podría resultar de la ausencia de seguridad.

Las áreas a considerar deben incluir:

- Segregación de instalaciones y/o funciones.
- Controles de acceso para archivos de los sistemas de información y las funciones.
- Validación de los datos de entrada.
- Creación y revisión regular de las pistas de auditoría para eventos importantes e intentos de acceso no autorizado.
- Procedimientos, documentación y capacitación para permitir que el sistema sea utilizado de manera segura por personal no especializado.
- Creación y almacenamiento de copias de seguridad de datos y del sistema.
- Recuperación de fallos, especialmente para aplicaciones de alta disponibilidad.
- Uso del cifrado de datos para proteger los datos del acceso no autorizado, ya sea durante la transmisión o el almacenamiento.
- Uso de firmas digitales para proporcionar autenticación de mensajes.
- Uso de controles formales de cambios para garantizar la realización de pruebas y la autorización de actualizaciones.
- Uso de controles de versiones para el software y la documentación del sistema de Información.
- Protección de los datos de prueba, asegurando que los datos de producción sean "despersonalizados" antes de su uso y retirados después de la prueba.
- Restricción en el acceso a las herramientas de auditoría del sistema, para evitar el uso indebido.

10. Planificación de la continuidad del negocio

Los planes de Continuidad de Negocios serán desarrollados, implementados y probados regularmente para proteger la información y los procesos de los efectos de grandes fallas o desastres.
Los propietarios de la información y de los sistemas de información determinarán la criticidad de la información sensible y de todos los sistemas de la empresa afán de preparar medidas apropiadas que garanticen la disponibilidad de los servicios.

Debe incluirse la identificación y reducción de riesgos, y la creación y prueba de procesos para reanudar las operaciones esenciales.
Los planes de continuidad deben enfocarse principalmente en mantener activos los procesos y servicios esenciales, incluyendo para ello personal y requerimientos no informáticos necesarios.

Cada plan debe especificar claramente las condiciones de su activación, los responsables para cada componente del plan y el responsable del plan en su conjunto.

El proceso de planificación de la continuidad debe abarcar:

- Determinación del impacto de falla.
- La concepción y el acuerdo sobre arreglos de emergencia.
- Documentación de procedimientos, procesos y responsabilidades.
- Preparación y mantenimiento de los activos redundantes (por ej. almacenamiento externo de las copias de seguridad, documentación y equipo).
- Capacitación del personal involucrado.
- Cronograma de pruebas para todos los componentes. Revisión y actualización del plan para que coincida con los cambios en el entorno o en el procesamiento de los sistemas.
- Comunicación con los usuarios afectados en caso de falla grave, incluyendo alternativas de comunicación electrónica.

11. Cumplimiento de los requisitos legales

Todos los requisitos contractuales y estatutarios pertinentes deben ser documentados y definidos explícitamente para cada sistema de información. Los controles y responsabilidades específicos para cumplir con estos requisitos deben ser documentados.
Los usuarios del software patentado deben ser conscientes de las limitaciones impuestas por los acuerdos de licencia y cumplir con los mismos.

Se debe mantener un registro de software para todos los sistemas de IT y se deben realizar auditorías de manera regular del uso del software.
Los usuarios no deben hacer copias del software de una computadora a otra sin la autorización de los propietarios del software.

ANEXO III

Procedimiento de Auditoria Interna

1. Objetivo

El objetivo de la auditoria interna es identificar, verificar y medir la eficacia del sistema implementado por la empresa con miras a realizar un correcto mantenimiento continuado y evolutivo del Sistema de Gestión de la Seguridad de la Información.

Este documento establece los lineamientos y los procedimiento a seguir para la planificación y realización de la auditoria interna del SGSI de la empresa, y así también los reportes de resultados de la evaluación

2. Alcance

Este procedimiento es aplicable a todas las auditorias de los procesos de la empresa enmarcados dentro del SGSI.

3. Perfil del auditor interno

Es importante garantizar la imparcialidad del equipo auditor en el proceso de auditoria. Ninguno de los miembros debe haber participado en la elaboración de manuales, políticas o procedimientos de una organización a la que se esta evaluado. Los auditores no pueden ser parte del grupo de toma de decisiones sobre el estado del SGSI, y tampoco pueden dar recomendaciones especificas para el desarrollo del SGSI.

El equipo auditor debe contar con las siguientes habilidades y regirse según el código de conducta que se especifican a continuación:

Habilidades y capacidades personales requeridas:

- Actitud ética, imparcial, sincera, honesta y discreta.
- Capacidad para el trabajo en equipo.
- Tener una actitud abierta y estar dispuesto a considerar ideas o puntos de vista alternativos.
- Mostrarse diplomático y hábil en las relaciones con la gente.
- Ser observador, constante y activamente consciente de los entornos físicos y las actividades.
- Ser perspicaz, instintivamente consciente y capaz de entender y adaptarse a las situaciones.
- Ser tenaz, persistente y orientado sobre la consecución de los objetivos.
- Tener poder de decisión, siendo capaz de alcanzar conclusiones oportunas basadas en el razonamiento lógico y el análisis.
- Mostrarse independiente en las actuaciones, relacionándose al mismo tiempo con otros de manera eficaz.

Código de conducta del equipo auditor

- Actuar de forma veraz e imparcial
- Evitar cualquier tipo de asignación que pueda cuásar conflicto de intereses
- No aceptar ningún tipo de incentivo, comisión, descuento u otro tipo de provecho por parte del auditado
- No revelar las observaciones de las auditorias a terceros
- No actuar de forma que pueda causar perjuicio a alguna de las partes interesadas

Los miembros del equipo de auditoria deben cumplir los siguientes requisitos:

Roles	Educación	Educación continuada	Experiencia
Auditor jefe	Diploma superior	• Haber aprobado y certificado un curso de entrenamiento como auditor de 24 horas • Haber aprobado un curso de fundamentos en sistemas de gestión de la calidad	Preferiblemente haber participado como observador en una auditoría mínimo de 8 horas.
Auditor Acompañante	Diploma superior	• Haber aprobado y certificado curso de entrenamiento como auditor de 24 horas • Haber aprobado curso de fundamentos en sistemas de gestión de la calidad	Preferiblemente haber participado como observador en una auditoría mínimo de 8 horas.
Experto técnico	Diploma superior en el área de la auditoria	• Preferiblemente formación continuada en el proceso auditar.	Un año de experiencia en el tema de auditoria.
Auditor en formación	Diploma superior	• Haber aprobado y certificado curso de entrenamiento como auditor de 24 horas • Haber aprobado curso de fundamentos en sistemas de gestión de la calidad	NA

4. Proceso general de la auditoria

Las 3 fases del procesos y sus actividades se muestran en la Ilustración 1

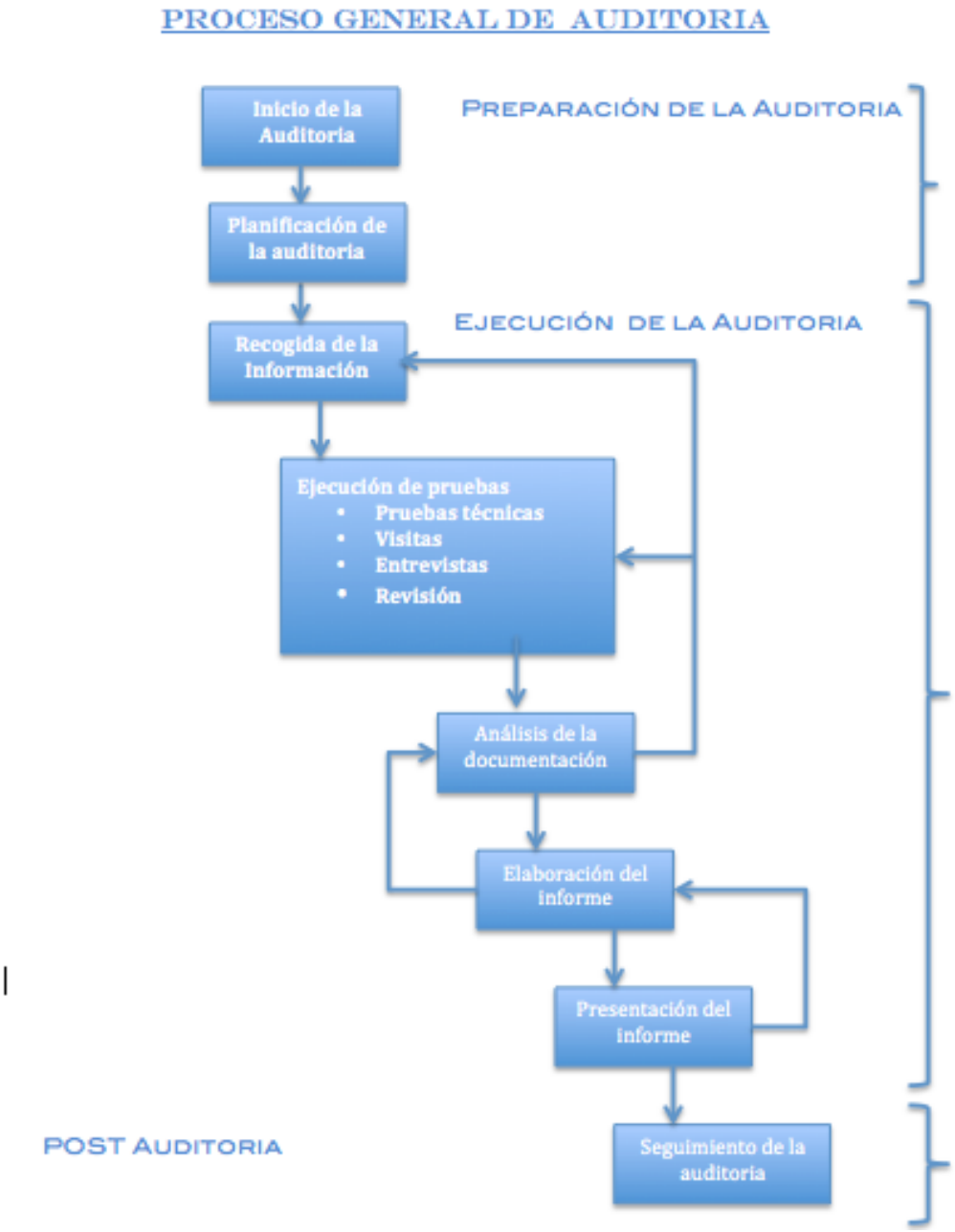


Ilustración 1: Fases Auditoria

I Preparación de la auditoría

Es la fase inicial del proceso de auditoría y en la que se realiza una primera reunión entre el auditor jefe, el director general y el responsable de seguridad de la empresa para establecer de una manera clara cuáles son los objetivos de la auditoría a realizar y lo que se espera de la misma.

Se determinarán los procedimientos de comunicación entre el equipo auditor y los responsables de la empresa.

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

Se definen las pruebas que se van a realizar durante el proceso de la auditoría.

II Ejecución de la auditoría

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

Las tareas son:

- Recolección de la información necesaria:
    - Recopilación de toda la información relevante para entender correctamente el entorno a auditar:
        - Los requisitos del negocio
        - Leyes y regulaciones.
    - Identificar cargos/roles/funciones para las entrevistas y el personal que deberá asistir:
        - La estructura organizacional
        - Los roles y las responsabilidades
    - La identificación y estudio de la documentación existente del auditados que sea relevante para la auditoria:
        - Políticas y procedimientos de seguridad.
        - Descripción de las medidas de control establecidas
        - Descripción de los entornos de tratamiento de la información y estudio de las vulnerabilidades conocidas que les sean aplicables.
- Ejecución de pruebas:
    - Se buscarán fallos en la documentación de la empresa.
    - Se realizarán entrevistas con el personal de la empresa.
    - Se ejecutarán las pruebas técnicas que se consideren oportunas.
    - Se realizan las visitas para constatar aspectos de seguridad física y/o comprobación in situ del funcionamiento de los sistemas de información.

- Elaboración del informe de auditoría.

III Informe de la auditoría

El informe de la auditoria es el documento que tiene los resultados y las conclusiones una vez realizadas las pruebas.

En este documento se especifican las no conformidades que se detectaron y las recomendaciones pertinentes.

A continuación se presentan modelos de documentos tanto para el programa, el plan y el informe de las auditoria.

INFORME DE AUDITORIA INTERNA

Fecha: / /

I DATOS DE LA AUDITORIA INTERNA			
N° DE AUDITORIA		**NORMA DE REF.**	
FECHA DE AUDITORIA			
LUGAR DE LA AUDITORIA			
II OBJETIVO DE LA AUDITORIA			
III ALCANCE DE LA AUDITORIA INTERNA			
IV. EQUIPO AUDITOR			
Auditor Jefe			
Auditores internos			
Auditores en formación			
V INVITADOS			
Expertos			
Observadores			
VI. FORTALEZAS Y DEBILIDADES			
FORTALEZAS		**DEBILIDADES**	
VII RESULTADOS DE LA AUDITORIA INTERNA			
No Conformidades:	Observaciones:	Oportunidades de mejora:	
No CONFORMIDADES			

N°	Área/ Proceso	Descripción	Responsable	Auditor
(Aumentar tantas líneas sean necesarias)				

OBSERVACIONES

N°	Área/ Proceso	Descripción	Responsable	Auditor
(Aumentar tantas líneas sean necesarias)				

OPORTUNIDADES DE MEJORA

N°	Área/ Proceso	Descripción	Responsable	Auditor
(Aumentar tantas líneas sean necesarias)				

PLAN DE AUDITORIA INTERNA
FECHA: / /

I DATOS DE LA AUDITORIA INTERNA			
N° DE AUDITORIA		NORMA DE REF.	
II OBJETIVO DE LA AUDITORIA			
III ALCANCE DE LA AUDITORIA INTERNA			
IV. EQUIPO AUDITOR			
Auditor Jefe			
Auditores internos			
Auditores en formación			
V INVITADOS			
Expertos			
Observadores			

VI PLAN DE AUDITORIA

Fecha	**Hora**	**Audit**	**Proceso/Área**	**Criterios de Auditoria**		
				Clausula/control	Documentación	Auditado
			Reunión de apertura			
			Reunión de cierre			

VII APROBACION DEL PLAN DE AUDITORIA	
Elaborado por:	**Aprobado por:**
Nombre, cargo y firma Fecha: / /	Nombre ,cargo y firma Fecha: / /

PROGRAMA ANUAL DE AUDITORIA

I DATOS GENERALES

Norma de referencia	Año :	
Objetivo		

II PROGRAMA DE AUDITORIAS

N°	Proceso/Área	Mes/Semanas																																															
		Ene				Feb				Mar				Abr				May				Jun				Jul				Ago				Sep				Oct				Nov				Dic			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	(agrega líneas si necesario)																																																
N° de Auditorias																																																	
Total de auditorias																																																	

II PROGRAMA DE AUDITORIAS

Elaborado por:	Aprobado por:
Nombre, cargo y firma	Nombre, cargo y firma
Fecha: / /	Fecha: / /

5 Programa de auditorias

En la Tabla 1: Programa de auditoria se detallan las auditorias programadas para los próximos 3 años.

PROGRAMA DE AUDITORIAS PARA LOS SIGUIENTES 3 AÑOS

Año	Proceso/Area	Mes/Semanas											
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	5. Políticas de seguridad												
	6. Aspectos organizativos de la seguridad de la información												
	7. Seguridad relativa a los recursos humanos												
	8. Gestión de activos												
	9. Control de accesos												
2	10. Criptografía												
	11. Seguridad física del entorno												
	12. Seguridad de las operaciones												
	13. Seguridad de las comunicaciones												
	14.Adquisición, desarrollo y mantenimiento de los sistemas de información												
3	15. Relaciones con proveedores												
	16. Gestión de incidentes de la seguridad de la información												
	17. Aspectos de seguridad de la información para la gestión de la continuidad de negocios												
	18. Cumplimiento												

Tabla 1: Programa de auditor

ANEXO IV

INDICADORES DEL SGSO

Controles	Indicador	Descripción	Formula de medida/Procedimiento	Tolerancia	Freq.
5.1.2, 14.2.1, 10.1.1, 9.1.1,10.2.9, 15.1.1, 13.2.1	Políticas de seguridad	Revisión de las políticas por parte de la dirección	Se verifica que se revise por lo menos una vez al año	=1	Anual
6.1	Organización Interna				
6.1.1.	Roles y Responsabilidades	Verificar que todas las responsabilidades están definidas y asignadas	roles y responsabilidades asignados/ total roles y responsabilidades	=1	Anual
6.1.2	Segregación de tareas	Las funciones y áreas de responsabilidad deben estar segregadas	Numero no conformidades identificadas	> 1	Anual
6.1.3	Contacto con las autoridades	Procedimientos implantados que especifiquen cuándo y cómo contactar las autoridades. Con quienes se puede contactar.	Numero no conformidades identificadas	< 1	Anual
6.1.5	Seguridad de la información en la gestión de proyectos	Integración de la seguridad de la información en los proyectos	(N° de proyectos que no abordan/ N° total de proyectos)*100	<=5%	Anual
6.2	Movilidad				
6.2.1	Dispositivos móviles	Respeto de la política y de las medidas de seguridad con respecto a la movilidad	(Numero de disp. móviles con incidentes/ numero total de dispositivos móviles)*100	<= 5%	Anual
6.2.2	Teletrabajo	Respeto de la política y de las medidas de seguridad con respecto al teletrabajo	(No de incidentes durante teletrabajo /No total de incidentes)	<=5%	Anual
7.1	Antes del empleo				
7.1.2	Términos y condiciones del empleo	Los términos y condiciones del trabajo reflejan la política de seguridad de la organización	(No de Contratos firmados con los términos y condiciones/No total de contratos)*100	> 95%	Anual
7.2	Durante el empleo				

7.2.2	Concienciación, educación y capacitación	Los empleados de la empresa han recibido capacitación y están consientes sobre la seguridad de la información	(No de empleados capacitados / No total de empleados)*100	>95%	Anual
7.3	Finalización del empleo o cambio				
7.3.1	Responsabilidad ante la finalización o cambio	Definir y comunicar las responsabilidades a los empleados al cese o al cambio	No de comunicaciones / No total de empleados en cese o cambio	> 0.9	Anual
8.1	Responsabilidad sobre los activos				
8.1.1	Inventario de activos	La información ha sido clasificada en términos de importancia y relevancia	(N° de activos no inventariados/ N° total activos) *100	<5%	Bienal
8.1.2	Propiedad de los activos	Los activos tienen un dueño	(N° de activos sin dueño/ N° total activos) *100	<5%	Anual
8.1.3	Uso aceptable de activos	El reglamento de uso aceptable de la información y de los activos son implementados	(N° de activos mal usados/ N° total activos) *100	<5%	Anual
8.1.4	Devolución de activos	Los activos se devuelven al finalizar la relación con la empresa	(N° de activos o devueltos / N° total de activos)*100	> 95%	Anual
8.2	Clasificación de la información				
8.2.1	Clasificación de la información	Clasificación de la información en términos de importancia	(N° de documentos clasificados / N° total de docs.)*100	> 95%	Anual
8.2.2	Etiquetado de la información	Existen procedimientos implantados para el etiquetado de la información de acuerdo a la clasificación	(N° de docs. etiquetados / N° total de docs. clasificados	>95%	Anual
8.2.3	Manipulación de la información	Existen procedimientos implantados para la manipulación de la información	(N° de incidentes de mala manipulación de la información/ N° total de docs. clasificados)*100	<5%	Semestre
8.3	Manejo de los medios				
8.3.1	Gestión de los medios removibles	Se implementan procedimientos para la gestión de acuerdo a la clasificación	(N° procedimientos medios removibles/ N° total de medios removibles)*100	>95%	Anual
8.3.2	Eliminación de los medios	Se usan procedimientos formales para eliminar los medios	(N° de medios eliminados sin un procedimientos formal/ N° total de medios eliminados	<5%	Anual

8.3.3	Transferencia física de los medios	Los medios con información se deben proteger contra los accesos no autorizados, adecuados o corrupción durante el transporte	(N° de medios no protegidos/ N° total de medios)*100	<5%	Semestral
9.1.2	Acceso a las redes y a los servicios de red	Los usuarios tienen acceso solo a las redes y servicios autorizados	(No de accesos no autorizados / no total de accesos)*100	<=1%	Trimestre
9.2	Gestión de acceso de usuario				
9.2.1	Registro y baja de usuario	Se debe implementar un proceso de registro y cancelación de registro de usuario	(N° registros/bajas sin el proceso /N° total de registros/bajas)*100	=1	Mensual
9.2.2	Asignación de acceso a usuario	Debe existir un procedimiento formal para la asignación(asignar/revocar) de accesos para todos los usuarios, todos los sistemas y servicios.	(N° de asignación sin respeto del procedimientos/N° total de asignaciones)*100	<=1%	Mensual
9.2.3	Gestión de derechos de accesos privilegiados	Se debe restringir y controlar la asignación y el uso de los derechos de acceso privilegiado	(N° de usuarios con acceso privilegiado/ N° total de usuarios activos)*100	<5%	Mensual
9.2.4	Gestión de la información secreta y autenticación de usuarios	Se debe controlar la asignación de información de autenticación secreta mediante proceso formal	(N° asignaciones mediante proceso formal / N° de asignaciones)*100	> 95%	Mensual
9.2.5	Revisión de los derechos de acceso de usuarios	Verificar que los derechos de acceso se modifican cada que un empleado cambia o se retira	N° de revisiones de los derechos por usuario	=1	
9.2.6	Eliminación o ajuste de los derechos de acceso	Retirar los derechos de acceso de todos los empleados y usuarios externos una vez que la relación con la empresa termina	(N° de usuarios con cambios en la relación laboral con la empresa y que no han sido actualizados / N° de usuarios con cambios en la relación laboral con la empresa)*100	<=1%	Anual
9.3.1	Uso de la información secreta de autentificación	Verificar que los empleados son responsables en el manejo de la información de autenticación	(No de usuario con incidentes del manejo de la información de autenticación / N° total de usuarios)*100	< 1%	Trimestre
9.4	Control de acceso				
9.4.1	Restricción de acceso a la información	Restringir el acceso a la información y a las funcione de acuerdo a la política de acceso	(No de accesos no autorizados / no total de accesos)*100	<1%	Mensual

9.4.2	Procedimiento de inicio de sesión seguro	Cuando se requiera el acceso debe ser controlados por un procedimientos de inicio y sesión seguro	(N° de aplicación sin el procedimiento implementado pero lo requieren / N° de aplicaciones que requieren el procedimiento)*100	<=1%	Semestral
9.4.3	Sistema de gestión de contraseña	Los sistemas de gestión de contraseñas deben ser interactivos y asegurar contraseñas de calidad	(N° de sistemas de gestión de contraseñas que no cumplen / n° de sistemas de gestión de contraseñas)*100	<=1%	Semestral
9.4.4	Uso de utilidades con privilegios del sistema	Restringir y controlar el uso de estas utilidades	(No de ordenadores con utilidades/ No total de ordenadores)*100	<=1%	Semestral
9.4.5	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas	Verificar que todos los usuarios que tienen acceso al código tienen razones justificadas		Mensual
10.1	Controles criptográficos				
10.1.2	Gestión de claves	Desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante su vida útil	Revisar la política por lo menos una vez al año	=1	Anual
11.1	Área Seguras				
11.1.1	Perímetro de seguridad física	Definir y utilizar perímetros de seguridad para proteger las áreas que contienen información sensible y las instalaciones de procesamiento de la información	(N° de áreas con perímetro de seguridad / N° de áreas a proteger)*100	>90%	Semestral
11.1.2	Controles de acceso físico	Las áreas seguras deben tener controles y solo las personas autorizadas deben ingresar	(N° de áreas a controlar sin controles establecidos / N° total de áreas a controlar)*100	< =1%	Semestral
11.1.3	Seguridad de oficinas, salas e instalaciones	Diseñar y aplicar la seguridad física en oficinas, salas y reuniones	(N° de ambientes sin protección y a proteger / N° total de ambientes a proteger)*100	< =1%	Semestral
11.1.4	Protección contra amenazas externas y del ambiente	Diseñar y aplicar la protección física contra danos por desastre natural, ataques o accidentes	Revisión de la protección física	=1	Anual

11.1.5	Trabajo en áreas seguras	Diseñar y aplicar procedimientos para trabajar en áreas seguras	(N° de usuarios que trabajan en áreas seguras con conocimiento de los procedimientos / N° total de usuarios que trabajan en áreas seguras)*100	>95%	
11.1.6	Áreas de entrega y carga	Controlar los puntos de acceso a las diferentes áreas de entrega y de carga y evitar accesos no autorizados	(N° de accesos no autorizados / N° total de accesos)*100	< =1%	Mensual
11.2	Equipamiento				
11.2.1	Ubicación y protección de equipos	Los equipos deben 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.	(N° de incidentes de equipos no protegidos / N° total de incidentes equipos) * 100	< =1%	Anual
11.2.2	Elementos de soporte	Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en el elemento de soporte	(N° de incidentes de protección de equipos / N° total de incidentes equipos)*100	<5%	Anual
11.2.3	Seguridad del cableado	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información deben ser protegidos contra la intercepción, interferencia o posibles daños.	(N° de incidentes protección cables)	<=2	Anual
11.2.4	Mantenimiento de los equipos	Los equipos deben mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.	N° de mantenimientos de los equipos	>=1	Anual
11.2.5	Retiro de materiales propiedad de la empresa	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.	(N° de equipos retirados son autorización / N° total de equipos retirados	>99%	Anual
11.2.6	Seguridad de los equipos fuera de las instalaciones	Se debe aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos	(N° de equipos fuera de la empresa con incidentes / N° total de equipos fuera de la empresa) *100	<90%	Anual

11.2.7	Reutilización o eliminación segura de equipos	Se deben verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.	(N° de equipos eliminados de manera segura / numero de equipos eliminados)*100	>95%	Anual
11.2.8	Equipo de usuario desatendido	Los usuarios se deben asegurar de que los equipos no supervisados cuentan con la protección adecuada.	(N° de veces que un usuario a desatendido su equipo)	<2	Anual
11.2.8	Política de puesto de trabajo despejado y pantalla limpia	Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	(N° de veces que un usuario no ha respetado ésta política)	<2	Anual
12.1	Procedimientos y responsabilidades operacionales				
2.1.1.	Documentación de procedimientos de las operaciones	Se deben documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.	(N° de proc de operación documentados / N° total de procedimientos de operación)*100	>95%	Anual
12.1.2	Gestión de cambios	Se deben controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información	N° de cambios en el sistema sin registro/N° total de cambios en el sistema)*100	>95%	Anual
12.1.3	Gestión de capacidades	Se debe monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.	Revisión de las proyecciones de capacidades	=1	Anual
12.1.4	Separación de los recursos de desarrollo, prueba y operaciones	Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.	Implantación de entornos diferentes ?	Si	Anual

12.2	Protección contra el software malicioso				
12.2.1	Controles contra el código malicioso	Evitar infecciones			
12.3	Copias de seguridad				
12.3.1	Copias de seguridad de la información	Se deben realizar copias regulares de la información, del software y de las imágenes del sistema en relación a una política de respaldo convenida.	N° de copias de respaldo ejecutadas exitosamente / N° total de copias de respaldo programadas)*100	>95%	Semestral
12.4	Registros y supervisión				
12.4.1	Registro de eventos	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.	(N° usuarios sin registro de eventos/ N° total de usuarios)*100	<=1%	Anual
12.4.2	Protección de la información de registro	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.	(N° de registros alterados / N° de registros) *100	<5%	Anual
12.4.3	Registros de administración y operación	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.	Sistema de registro de actividades del administrados y operadores activos. No de revisiones de los registros	>=1	Anual
12.4.4	Sincronización del reloj	se deben sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.	(No de relojes sincronizados / N° de sistemas de procesamiento a sincronizar)	>95%	Anual
12.5	Control del software en explotación				
12.5.1	Instalación del software en explotación	Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.	(N° de instalaciones no autorizadas / N° total de instalaciones)*100	<10%	Anual
12.6	Gestión de Vulnerabilidad técnica	e debería obtener información sobre las vulnerabilidades técnicas de los sistemas de			

		información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.			
12.6.2	Restricción en la instalación de software	Verificar que el software que se instala se encuentra dentro del software permitido	No de software instalado non conforme a la directica por ordenador	< = 1	Anual
12.6.2	Restricción en la instalación del software	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.	Revisión de las reglas y la implantación		Anual
12.7	Consideraciones sobre la auditoria de sistemas de información				
12.7.1	Controles de auditoria de sistemas de información	Se deberían planificar y acordar los requisitos y las actividades de auditoria que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.	Plan de auditoria aprobado	=1	Anual
13.	Seguridad de las comunicaciones				
13.1	Gestión de la seguridad de redes				
13.1.1	Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.	(N° de incidentes relacionados con la protección de la información	<=2	Mensual
13.1.2	Seguridad de los servicios de red	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.	N° de acuerdos SLA que no incluyen los mecanismos de seguridad / N° total de acuerdos SLA)*100	<=5%	Anual
13.1.3	Segregación en redes	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.	Verificación de la segregación	=1	Anual

13.2	Intercambio de información				
13.2.2	Acuerdos de transferencia de información	Identificar, documenta y Revisar los requisitos de los acuerdos de confidencialidad	(No comunicaciones externas protegidas/No comunicaciones externas totales)*100	>90%	Anual
13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información referida en la mensajería electrónica	(No comunicaciones externas protegidas/No comunicaciones externas totales)*100	>90%	anual
13.2.4	Acuerdos de confidencialidad o no revelación	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.	Revisar los acuerdos de confidencialidad	=1	Anual
14.1	Requisitos de seguridad en sistemas de información				
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.	(N° sistemas que incluyen los requisitos / numero total de sistemas)*100	>95%	Anual
14.1.2	Asegurar los servicios de aplicaciones en redes publicas	La información de los servicios de aplicación que pasan a través de redes publicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.	N° de incidentes de protección en redes publicas	<=2	Semestral
14.1.3	Protecciones de las transacciones de servicios de aplicaciones	Se debe proteger la información en transacciones de servicios de aplicación para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.	N° de incidentes relacionados con las transacciones de una aplicación	<=2	Semestral
14.2	Seguridad en el desarrollo y en los procesos de soporte				
14.2.1	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.	revisión de la política	=1	Anual

14.2.2	Procedimiento de control de cambios en el sistema	En el ciclo de vida de desarrollo se debe hacer uso de procedimientos formales de control de cambios.	(N° de cambios ejecutados sin procesos formales / N° total de cambios) *100	<= 5%	Semestral
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Las aplicaciones criticas para el negocio se deben revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.	Revisión del plan de revisiones técnicas implantado	=1	Semestral
14.2.4	Restricciones a los cambios en los paquetes de software	Se debe evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.	(N° de cambios no autorizados / N° total de cambios)*100	<= 5%	Anual
14.2.5	Principios de ingeniería de sistemas seguros	Se debe establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.	(No de sistemas que no aplican principios de seguridad / No total de sistemas)*100	<= 5%	Anual
14.2.6	Entorno de desarrollo seguro	Las organizaciones debe establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.	N° de accesos no autorizados a los entornos de desarrollo	<=2	Anual
14.2.7	Externalización del desarrollo de software	a organización debe supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.	auditorias		
14.2.8	Pruebas funcionales de seguridad del sistema	Se debe realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.	(N° de sistemas en desarrollo con pruebas funcionales de seguridad establecidas / N° de sistemas en desarrollo)*100	>95%	Anual
14.2.9	pruebas de aceptación del sistema	Se debe establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones	(N° de sistemas aceptados con pruebas de aceptación implementados / N° de sistemas aceptados)*100	>95%	Anula
14.3	Datos de prueba				

14.3.1	Protección de los datos de prueba	Proteger y controlar los datos de prueba	(No de aplicación con datos de prueba protegidos y controlados / No total de aplicaciones en prueba)*100	<10%	Anual
15.1	Seguridad en las relaciones con los proveedores				
15.1.2	Requisitos de seguridad en contratos con terceros	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.	No incumplimientos SLA / No total SLA * 100	<= 5%	Anual
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.			
15.2	gestión de la provisión de los servicios del proveedor				
15.2.1	Control y revisión de la provisión de servicios del proveedor	Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.	Auditoria de los proveedores	=1	Anual
15.2.2	Gestión de cambios en la provisiones del proveedor	Se debe administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.	Revisión de las políticas en función a los cambios de provisión de los proveedores	=1	Anual
16.1	Gestión de Incidentes de Seguridad				

16.1.2	Notificación de los eventos de seguridad de la información	Notificar los eventos de seguridad por los canales y lo antes posible	(No de incidentes no notificados por los canales / No total de incidentes)*100	<10%	Anual
16.1.3	Notificación de puntos débiles de la seguridad	Se debe requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.	No de notificaciones de puntos débiles		Anual
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Se debe evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.	(N° de eventos sin clasificación / N° total de eventos)*100	<5%	Anual
16.1.5	Respuesta a los incidentes	Responder a los incidentes de acuerdo a los procedimientos establecidos	(No de respuestas sin procedimiento/ N° total de respuestas)*100	>95%	Anual
16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se reutilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.	N° de incidentes anteriores que se repiten por sistema	<=2	Anual
16.1.7	Recopilación de evidencias	La organización debe definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.	N° de incidentes sin evidencias / N) total de incidentes)*100	>95%	Anual
17.1	Continuidad de la seguridad de la información				
17.1.2	Implementar la continuidad de la seguridad de la información	Establecer e implementar procesos, procedimientos y controles para asegurar la continuidad de la seguridad de la Información	No de procesos de continuidad funcionando/ No total de procesos de continuidad	>95%	Anual
17.1.1	Planificación de la continuidad de la seguridad de la información	Controlar que los controles son validos y eficaces	(No de controles ineficaces / No total de controles)*100	<=1%	Semestral

17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Se debe verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones	Verificación de los controles de continuidad	=1	Semestral
17.2	Redundancias				
17.2.1	Disponibilidad de los recursos de tratamientos de la información	Se debe implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.	N° de pruebas de disponibilidad con los sistemas redundantes	=1	Anual
18.1	Cumplimiento de los requisitos legales y contractuales				
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se deberían identificar, documentar y mantener al día de manera explicita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.	Revisión de los requisitos estatutarios, normativos y contractuales legislativos	=1	Semestral
18.1.2	Derechos de propiedad intelectual	Debe implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software propietario.	(N° de personas en la empresa que no conocen los procedimientos / N° de personas que trabajan en la empres)*100	<5%	Anual
18.1.3	Protección de los registros de la organización	os registros se deberían proteger contra perdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.	N° de perdidas de registros de la organización	<=1	Anual

18.1.4	Protección y privacidad de la información de carácter personal	Se debe garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables	N° de incidentes con relación a la LOPD debe tender a cero	<=1	Anual
18.1.5	Regulación de los controles criptográficos	Se debe utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.	N° de incidentes con relación a la regulación de controles criptographicos debe tender a cero	<=1	anual
18.2	Revisiones de la seguridad de la información				
18.2.1	Revisiones independientes de la seguridad de la información	Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.	N° de auditorias	1	Bienal
18.2.2	Cumplimiento de las políticas y de las normas de seguridad	Se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.	N° de Revisiones de las políticas	1	Anual
18.2.3	Comprobación del cumplimiento técnico	Verificar el cumplimiento de los sistemas de información en cuanto a las políticas y normas	N° de auditorias	1	Anual

ANEXO V

DECLARACION DE APLICABILIDAD

Control	Aplica	Implementaciones	Documentos
5 POLÍTICAS DE SEGURIDAD			
5.1 Directrices de la Dirección en seguridad de la información			
5.1.1 Conjunto de políticas para la seguridad de la información	Si	Aprobado por la dirección y comunicado al personal	Política de Seguridad
5.1.2 Revisión de las políticas para la seguridad de la información	Si	Existe un informe de revisión del año anterior	Actas e informes de revisión
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1 Organización interna			
6.1.1 Asignación de responsabilidades para la seguridad de la información	Si	Los roles y responsabilidades están definidas y existe personal asignado	Actas de nombramiento
6.1.2 Segregación de tareas	Si	Las tareas se asignan según las responsabilidades	Actas de nombramiento
6.1.3 Contacto con las autoridades	Si	Existe un directorio de las autoridades pertinentes Existen procedimientos para el contacto de autoridades	Actas de nombramiento
6.1.4 Contacto con grupos de interés especial	Si	Existe evidencia de inscripciones a grupos de interés	Certificaciones
6.1.5 Seguridad de la información en la gestión de proyectos	Si	Existe documento de recomendación	Actas de nombramiento
6.2 Dispositivos para movilidad y teletrabajo			
6.2.1 Política de uso de dispositivos para movilidad	Si	Existe un documento con recomendaciones y guías	Política de seguridad
6.2.2 Teletrabajo	Si	Existe un documento con recomendaciones y guía	Política de seguridad

7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS			
7.1 Antes de la contratación			
7.1.1 Investigación de antecedentes	Si	Forma parte del proceso de contratación de personal	Certificado de buena conducta
7.1.2 Términos y condiciones de contratación	Si	Existe una clausula en el contrato que aborda la seguridad de la información	Política de seguridad Contratos
7.2 Durante la contratación			
7.2.1 Responsabilidades de gestión	Si	Esta responsabilidad esta asignada al equipo de RRHH	Informes de auditorias
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Si	Se organizan regularmente talleres de concientización de acuerdo a grupos cibles.	Plan de formación Sesiones de información
7.2.3 Proceso disciplinario	Si	Existe un procedimiento disciplinario definido	Política de seguridad
7.3 Cese o cambio de puesto de trabajo			
7.3.1 Cese o cambio de puesto de trabajo	Si	Existe un procedimiento definido de cese y cabio de puesto de trabajo	Política de seguridad
8. GESTIÓN DE ACTIVOS			
8.1 Responsabilidad sobre los activos			
8.1.1 Inventario de activos	Si	Existe un inventario de los principales activos	Inventario de activos
8.1.2 Propiedad de los activos	Si	La propiedad esta reflejada en el inventario	Inventario de activos
8.1.3 Uso aceptable de los activos	Si	Existe un procedimiento de uso activos aprobado pero no siempre utilizado.	Política de seguridad
8.1.4 Devolución de activos	Si	Esta incluido dentro del procedimiento de uso de activos	Política de seguridad
8.2 Clasificación de la información			
8.2.1 Directrices de clasificación	Si	Existe procedimientos de uso de activos	Manual de clasificación
8.2.2 Etiquetado y manipulado de la información	Si	Existe procedimientos de uso de activos	Manual de clasificación
8.2.3 Manipulación de activos	Si	Existe procedimientos de uso de activos	Política de seguridad
8.3 Manejo de los soportes de almacenamiento			
8.3.1 Gestión de soportes extraíbles	Si	Existe procedimientos de uso de activos	Política de seguridad

8.3.2 Eliminación de soportes	Si	Existe procedimientos de uso de activos	Política de seguridad
8.3.3 Soportes físicos en tránsito	Si	Existe procedimientos de uso de activos	Política de seguridad
9. CONTROL DE ACCESOS			
9.1 Requisitos de negocio para el control de accesos			
9.1.1 Política de control de accesos	Si	Existe un documento de control de acceso aprobado y distribuido al personal	Gestión de control de accesos
9.1.2 Control de acceso a las redes y servicios asociados	Si	Existen procedimientos aprobados y en funcionamiento	Gestión de operaciones
9.2 Gestión de acceso de usuario			
9.2.1 Registro de acceso y baja de usuarios	Si	Existen procedimientos aprobados y en funcionamiento	Gestión de control de accesos
9.2.2 Provisión de acceso de usuario	Si	Existe un registro de los accesos y gestionado por el dpto. de IT e infraestructura	Gestión de control de accesos
9.2.3 Gestión de privilegios de acceso	Si	Existe un registro de los accesos y gestionado por el dpto. de IT e infraestructura	Gestión de control de accesos
9.2.4 Gestión de la información secreta de autenticación de los usuarios	Si	Existe un registro de los accesos y gestionado por el dpto. de IT e infraestructura	Gestión de control de accesos
9.2.5 Revisión de los derechos de acceso del usuario	Si	Existen procedimientos aprobados y en funcionamiento	Gestión de control de accesos
9.2.6 Retiro y/o reasignación de los derechos de acceso	Si	Existen procedimientos aprobados y en funcionamiento	Gestión de control de accesos
9.3 Responsabilidades del usuario			
9.3.1 Uso de la información secreta de la autenticación	Si	Existe una directiva sobre el uso y existe un mecanismo de implementación en funcionamiento	Política de seguridad
9.4 Control de acceso a sistemas y aplicaciones	Si		
9.4.1 Restricción de acceso a la información	Si	Existen procedimientos y controles implementados	Gestión de control de accesos
9.4.2 Procedimientos seguros de inicio de sesión	Si	Existen procedimientos y controles parcialmente implementados	Gestión de control de accesos
9.4.3 Sistema de gestión de contraseñas	Si	Existe un procedimiento implementado y comunicado	Gestión de control de accesos

9.4.4 Uso de utilidades con privilegios del sistema	Si	Existen procedimientos y controles implementados	Política de seguridad
9.4.5 Control de acceso al código fuente de los programas	Si	Existe un registro de los accesos y gestionado por el dpto. IT	Gestión de control de accesos
10. CRIPTOGRAFIA			
10.1 Controles criptográficos			
10.1.1 Política de uso de los controles criptográficos	SI	Existe procedimiento implantado por el dpto. IT	Política de seguridad
10.1.2 Gestión de claves	No	Existe un registro de acceso y gestionado por el dpto.. IT	Política de seguridad
11. SEGURIDAD FISICA DEL ENTORNO			
11.1 Áreas seguras			
11.1.1 Perímetro de seguridad física	Si	Las medidas de seguridad están definidas e implantadas en la empresa	Gestión de la seguridad física
11.1.2 Controles físicos de entrada	Si	Existen medidas de control físicas implantadas	Gestión de la seguridad física
11.1.3 Seguridad de oficinas, despachos y recursos	Si	Existen medidas de control físicas implantadas	Política de seguridad Gestión de la seguridad física
11.1.4 Protección contra las amenazas externas y ambientales	Si	Existen medidas de control físicas implantadas	Gestión de la continuidad del negocio
11.1.5 El trabajo en áreas seguras	Si	Existen medidas de control físicas implantadas	Gestión de la seguridad física
11.1.6 Áreas de carga y descarga	Si	Las áreas están delimitadas e identificadas	Gestión de la seguridad física
11.2 Seguridad de los equipos			
11.2.1 Emplazamiento y protección de equipos	Si	Existe un reglamento sobre la protección de equipos	Política de seguridad Gestión de la seguridad física
11.2.2 Instalaciones de suministro	Si	Los suministros están instalados y en funcionamiento	Gestión de la continuidad del negocio
11.2.3 Seguridad del cableado	Si	Existe un reglamento sobre la seguridad del cableado	Gestión de la seguridad física

11.2.4 Mantenimiento de los equipos	Si	Existe un procedimiento y un cronograma de mantenimiento de los equipos	Gestión de la continuidad del negocio
11.2.5 Salida de materiales propiedad de la empresa	Si	Existe un reglamento y procedimiento para la salida de materiales	Política de seguridad Gestión de la seguridad física
11.2.6 Seguridad de los equipos fuera de las instalaciones	Si	Existe una política de uso de los activos de la empresa	Política de seguridad Gestión de la seguridad física
11.2.7 Reutilización o eliminación segura de equipos	Si	Existe una política de uso de los activos de la empresa	Política de seguridad
11.2.8 Equipo de usuario desatendido	Si	Existe una política de uso de los activos de la empresa	Política de seguridad
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Si	Existe una política de uso de los activos de la empresa	
12. SEGURIDAD DE LAS OPERACIONES			
12.1 Procedimientos y responsabilidades operacionales	Si		
12.1.1 Documentación de procedimientos de las operaciones	Si	Existen documentos de los procedimientos y manuales de operación	Gestión de operaciones
12.1.2 Gestión de cambios	Si	Existen procedimientos definidos para la gestión de los Cambios	Gestión de operaciones
12.1.3 Gestión de capacidades	Si	Existe un procedimiento para la gestión de capacidades	Gestión de operaciones
12.1.4 Separación de los recursos de desarrollo, prueba y operaciones	Si	Los diferentes entornos de trabajo implementados	Gestión de operaciones
12.2 Protección contra el software malicioso			
12.2.1 Controles contra el código malicioso	Si	Existen procedimientos de control definidos e implantados	Políticas de seguridad Gestión de operaciones
12.3 Copias de seguridad			
12.3.1 Copias de seguridad de la información	Si	Existe procedimientos de copias de seguridad definidos e implantados	Gestión de operaciones
12.4 Registros y supervisión			
12.4.1 Registro de eventos	Si	Existen procedimientos definidos de uso de	Gestión de control de

		entornos e implantados	accesos Políticas de seguridad
12.4.2 Protección de la información de registro	Si	Existen procedimientos definidos de uso de entornos e implantados	Gestión de control de accesos Políticas de seguridad
12.4.3 Registros de administración y operación	Si	Existen procedimientos definidos de uso de entornos e implantados	Gestión de control de accesos Políticas de seguridad
12.4.4 Sincronización del reloj	Si	Existen procedimientos definidos de uso de entornos e implantados	Gestión de operaciones Políticas de seguridad
12.5 Control del software en explotación			
12.5.1 Instalación del software en explotación	Si	Existen procedimientos definidos de uso de entornos e implantados	Gestión de operaciones Políticas de seguridad
12.6 Gestión de la vulnerabilidad técnica	Si		
12.6.1 Gestión de la vulnerabilidad técnica	Si	Existen procedimientos definidos de uso de entornos e implantados	
12.6.2 Restricción en la instalación del software	Si	Existen procedimientos definidos de uso de entornos e implantados	Gestión de operaciones Políticas de seguridad
12.7 Consideraciones sobre la auditoria de sistemas de información			
12.7.1 Controles de auditoria de sistemas de información	Si	Existen procedimientos definidos de uso de entornos e implantados	Gestión de operaciones
13. Seguridad de las comunicaciones			
13.1 Gestión de la seguridad de redes			
13.1.1 Controles de red	Si	Existen controles definidos e implantados. Definidos en un documento resumido de uso aceptable de recursos	Gestión de operaciones Políticas de seguridad
13.1.2 Seguridad de los servicios de red	Si	Existen procedimientos de uso de entornos	Gestión de operaciones Políticas de seguridad
13.1.3 Segregación en redes	Si	Existen procedimientos de uso de entornos	Gestión de operaciones Políticas de seguridad
13.2 Intercambio de información			

13.2.1 Políticas y procedimientos en intercambio de información	Si	Existen lineamientos de uso aceptable de los recursos	Gestión de operaciones Políticas de seguridad
13.2.2 Acuerdos de intercambio de información	Si	Existen lineamientos de uso aceptable de los recursos	Gestión de la seguridad Políticas de seguridad
13.2.3 Mensajería electrónica	Si	Existen lineamientos de uso aceptable de los recursos	Gestión de la seguridad Políticas de seguridad
13.2.4 Acuerdos de confidencialidad o no revelación	Si	Existen lineamientos sobre la confidencialidad	Gestión de operaciones Políticas de seguridad
14. Adquisición, desarrollo y mantenimiento de los sistemas de información			
14.1 Requisitos de seguridad en sistemas de información			
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Si	Existen requisitos y controles de seguridad	Gestión de operaciones Políticas de seguridad
14.1.2 Asegurar los servicios de aplicaciones en redes publicas	Si	Existen procedimientos se seguridad implantados	Gestión de operaciones Políticas de seguridad
14.1.3 Protecciones de las transacciones de servicios de aplicaciones	Si	Existen mecanismos de protección de transacciones implantados	Gestión de operaciones Políticas de seguridad
14.2 Seguridad en el desarrollo y en los procesos de soporte			
14.2.1 Política de desarrollo seguro	Si	Existe procedimientos y guías de desarrollo de aplicaciones	Gestión del desarrollo
14.2.2 Procedimiento de control de cambios en el sistema	Si	Existe procedimientos y guías de gestión de cambios de aplicaciones	Gestión del desarrollo
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Si	Existe procedimientos y guías de gestión de cambios de aplicaciones	Gestión del desarrollo
14.2.4 Restricciones a los cambios en los paquetes de software	Si	Existe procedimientos y guías de gestión de cambios de aplicaciones	Gestión del desarrollo
14.2.5 Principios de ingeniería de sistemas seguros	Si	Existe procedimientos y guías de gestión de cambios de aplicaciones	Gestión del desarrollo
14.2.6 Entorno de desarrollo seguro	Si	Existen entornos propios de desarrollo	Gestión del desarrollo
14.2.7 Externalización del desarrollo de software	Si	Existen procedimientos y entornos para desarrollo externo	Gestión del desarrollo
14.2.8 Pruebas funcionales de seguridad del	Si	Existe procedimientos y guías para el procesos	Gestión del desarrollo

sistema		de pruebas	
14.2.9 pruebas de aceptación del sistema	Si	Existen procedimientos para la aceptación	Gestión del desarrollo
14.3 Datos de prueba	Si		
14.3.1 Protección de los datos de prueba	Si	Existe una normativa para el manejo de datos de test	Gestión del desarrollo Políticas de seguridad
15. RELACIONES CON PROVEEDORES			
15.1 Seguridad en las relaciones con los proveedores			
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Si	Existen procedimientos implantados	Gestión proveedores Políticas de seguridad
15.1.2 Requisitos de seguridad en contratos con terceros	Si	Existen lineamientos para compras/cambios con proveedores	
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	Si	Existen un conjunto de requisitos definidos	Gestión proveedores
15.2 gestión de la provisión de los servicios del proveedor			
15.2.1 Control y revisión de la provisión de servicios del proveedor	Si	Se solicitan reportes de auditorias a los proveedores	Gestión proveedores
15.2.2 Gestión de cambios en la provisiones del proveedor	Si	Se solicitan reportes gestión de cambios	Gestión proveedores
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION			
16.1 Gestión de incidentes de seguridad de la información y mejoras			
16.1.1 Responsabilidades y procedimientos	Si	Las responsabilidades no están claramente asignadas	Gestión de roles y responsabilidades Gestión de incidentes
16.1.2 Notificación de los eventos de seguridad de la información	Si	Existen procedimientos para las notificaciones	Gestión de incidentes Política de seguridad
16.1.3 Notificación de puntos débiles de la seguridad	Si	Recomendaciones de auditorias internas	Gestión de incidentes Política de seguridad
16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	Si	Resultados de auditorias	Gestión de incidentes

16.1.5 Respuesta a incidentes de seguridad de la información	Si	Existen procedimientos de respuesta a ciertos incidentes	Gestión de incidentes
16.1.6 Aprendizaje de los incidentes de seguridad de la información	Si	Existen algunas recomendaciones de auditorias anteriores	Gestión de incidentes
16.1.7 Recopilación de evidencias	Si	Existen procedimientos para la recopilación de evidencias pero	Gestión de incidentes
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS			
17.1 Continuidad de la seguridad de la información			
17.1.1 Planificación de la continuidad de la seguridad de la información	Si	Existen procedimientos definidos a ser implementados	Gestión de la continuidad del negocio
17.1.2 Implementar la continuidad de la seguridad de la información	Si	Existe un plan de continuidad implantado	Gestión de la continuidad del negocio
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si	Existe un plan de verificación de la continuidad	Gestión de la continuidad del negocio
17.2 Redundancias			
17.2.1 Disponibilidad de los recursos de tratamientos de la información	Si	Una arquitectura redundante esta implantada	Gestión de la continuidad del negocio
18. CUMPLIMIENTO			
18.1 Cumplimiento de los requisitos legales y contractuales			
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Si	Existe una normativa definida y implantada	Documento de legislación
18.1.2 Derechos de propiedad intelectual	Si	Existe un reglamentación sobre la propiedad intelectual	Propiedad intelectual
18.1.3 Protección de los registros de la organización	Si	Existe un procedimiento de protección de los registros.	Procedimiento de registros
18.1.4 Protección y privacidad de la información de carácter personal	Si	La política de privacidad y protección de la información de carácter personal esta desarrollada e implantada	Política de protección de datos
18.1.5 Regulación de los controles criptográficos	Si	Existen directivas para los controles en la transferencia de la información	Gestión de operaciones y comunicaciones

18.2 Revisiones de la seguridad de la información			
18.2.1 Revisiones independientes de la seguridad de la información	Si	Existe un plan de revisión independiente	Procedimientos de auditoria
18.2.2 Cumplimiento de las políticas y de las normas de seguridad	Si	Existen procedimientos de revisión y de medición	Actas de las reuniones de revisión
18.2.3 Comprobación del cumplimiento técnico	Si	Existen procedimientos para la verificación del cumplimiento	Procedimientos de auditoria

ANEXO VI

Procedimiento Revisión por Dirección

1 Introducción

La dirección de la empresa toma a cargo la revisión del SGSI. Es a través de esta revisión que la dirección busca garantizar que el Sistema de Gestión de Seguridad de la Información funcione de manera segura, continua y de mejoramiento continuo .

La revisión incluye la evaluación de las oportunidades de mejora y la necesidad de realizar cambios en el SGSI. En esta revisión se incluye la política de seguridad de la información y los objetivos de seguridad de la información.

2 Objetivo

El objetivo de este documentos es especificar el conjunto de acciones que la Dirección de la empresa debe realizar en el proceso de revisión de los procedimientos y los controles implementados.

3 Alcance

La revisión cubre el SGSI en su totalidad

4 Proceso de la revisión

La revisión será realizada por un comité de revisión que estará compuesto por el responsable de la seguridad de la información, el director de recursos humanos y los altos directivos de la empresa.

Esta revisión se realizara una vez al año.

En estas reuniones no participa el Director general debido a que no está interesado en los aspectos operacionales.

Se fija una reunión anual separada con el Director general para proporcionarle una visión general de alto nivel del estado de funcionando el sistema.

Para realizar esta revisión es necesario contar con la siguiente información :

1. Resultado de las revisiones anteriores
2. Un reporte de los cambios en los asuntos externos e internos pertinentes al SGSI
3. Retroalimentaciones sobre:
    a. las conformidades y acciones correctivas

    b. resultados de monitoreo y mediciones
    c. resultados de auditorias
    d. el cumplimiento de los objetivos de la seguridad de la información
4. Retroalimentación de todas las partes interesadas e involucradas.
5. Los resultados obtenidos de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.
6. Las oportunidades para la mejora continua

Los resultados de esta revisión deben incluir decisiones o acciones que estén relacionadas:

1. Con las oportunidades de mejora continua
2. Mejoras en la eficacia del SGSI
3. Actualización del plan de evaluación de riesgos y del tratamiento de riesgos
4. Necesidades de cambios al SGSI (procesos y controles)
5. Necesidades de recursos

Los resultados obtenidos de las revisiones serán documentados y registrados en las actas de las reuniones

Acciones de la agenda de la reunión de la revisión

1. Introducción
    a. Propósito de la reunión
    b. Revisión de la lista de asistentes, se debe tener la certeza de que las personas clave estén presentes.
2. Acciones de revisión de las Actas
    a. Revisión de actas de reuniones anteriores
    b. Verificar el estado de las acciones con los asistentes
    c. Registro del estado actual del SGSI frente a las acciones en curso
    d. Cierre de las acciones completadas
3. SGSI y Gestión de Riesgos
    a. Revisar / confirmar el alcance y los objetivos del SGSI
    b. Revisar el desempeño del SGSI y la mejora continua
    c. Revisar restricciones de recursos, presupuestos y otras cuestiones
    d. Revisar el registro de riesgos y los riesgos abiertos / cerrados
    e. Discutir políticas y procedimientos de seguridad de la información
4. Métricas de rendimiento / KPI
    a. Revisar métricas de rendimiento y KPI
    b. Discutir los resultados de incidentes recientes y respuesta
5. Reunión Cierre
    a. Confirmar las acciones y los propietarios de las acciones
    b. Confirmar plazos para acciones
    c. Confirmar fecha y hora de la próxima reunión, propósito, los participantes, los temas a tratar .
    d. Otros

A continuación se dispones de los documentos a ser utilizados para la reunión de revisión de la dirección y las actas de las reuniones.

AGENDA DE LA REUNIÓN DE REVISIÓN Y ACTA DE LA REUNIÓN

REUNION DE REVISION DE LA DIRECCION
REV: 00XXAAAA

PARTICIPANTES

Nombre	Titulo/Función	Presente
	SECURITY OFFICER	✔
	DIRECTOR DE RECURSOS HUMANOS	✔
	DIRECTOR DE OPERACIONES	

Fecha	Hora	Lugar

Presidente reunión	Moderador	Secretario actas	Expositor

PREPARACIÓN:	- - -
ENTRADAS:	- - - -
OBJETIVO	

TEMAS AGENDA	**1.**
	2.
	3.
	4.
	5
	6.
	7.
	8.
	9.
	10.

PROXIMA REUNION

Fecha	Hora	Lugar

Presidente reunión	Moderador	Secretario actas	Expositor

ACTA DE LA REUNION DE REVISION FECHA: / /

ITEM AGENDA	RESULTADOS/DECISIONES	ACTION A EJECUTAR, COMUNICACIONES	RESPONSABLE	DUE DATE	STATUS
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
(Aumentar líneas si necesario)					

RESUMEN DE RESULTADOS DE LA REUINION

Fecha de la siguiente reunión: / /

Firma: …… Fecha: / / **Firma: …… Fecha: / /**

Director de la reunión **Representante de la Dirección**

ANEXO VII

Gestión de Roles y Responsabilidades

La alta dirección de la empresa crea una estructura interna con responsabilidad directa sobre la seguridad de la información. Esta estructura interna describe los diferentes roles dentro de la seguridad de la información. Se especifican de manera clara cada una de las funciones y las responsabilidades por cada rol. Cada rol es asignado y comunicado a personas concretas en la compañía.

Esta estructura organizativa y sus funciones son aprobadas y apoyadas por la dirección.

Los roles y responsabilidades del personal que forma parte de esta estructura interna con responsabilidad directa sobre la seguridad de la información se detallan en las tablas que siguen a continuación.

Órganos definidos	Funciones	Miembros	Resumen
Comité de Dirección	• Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía. • Nombrar a los miembros de un Comité de Seguridad de la Información y darles soporte, dotarles de los recursos necesarios y establecer sus directrices de trabajo. • Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información. • Determinar el umbral de riesgo aceptable en materia de seguridad. • Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas. • Aprobar el Plan de seguridad de la información, que incluye los principales proyectos e iniciativas en la materia. • Realizar el seguimiento del cuadro de mando de la seguridad de la información.	• Director General • Director RRHH • Director financiero • Director Operaciones • Director de Comercializaciones • Director de Información • Director Riesgos	• Visión Estratégica • Aporte de recursos
Comité de la Seguridad de la Organización	• Implantar las directrices del Comité de Dirección. • Asignar roles y funciones en materia de seguridad. • Presentar para la aprobación al Comité de Dirección las políticas, normas y	Miembros permanentes • Security Officer	Responsable de las decisiones en materia de la seguridad de la

	responsabilidades en materia de seguridad de la información. • Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI). • Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Además de supervisar y hacer el seguimiento de su implantación. • Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio. • Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación. • Promover la concienciación y formación de usuarios y liderar la comunicación necesaria. • Revisar los incidentes más destacados. • Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.	• Director de Informaciones • Director de RRHH • Director Riesgos • Director Financiero • Director de Operaciones Miembros Invitados • Varia según la temática	información
Responsable de la Seguridad de la Información	• Implantar las directrices del Comité de Seguridad de la Información de la compañía. • Elaborar, promover y mantener una política de seguridad de la información, y proponer anualmente objetivos en materia de seguridad de la información. • Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el departamento de Administración y Finanzas.	Security Officer	Coordinación de las acciones orientadas a garantizar la seguridad de la informaciones y de proteger durante todo el ciclo de vida en términos de confidencialidad,

	• Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento. • Actuar como punto focal en materia de seguridad de la información dentro de la compañía a fin de gestionar la seguridad de la información de forma global. • Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo. • Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones. • Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. • Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio. • Velar por el cumplimiento legal coordinando las actuaciones necesarias con las unidades responsables. • Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad y hacer el seguimiento de los incidentes de seguridad. • Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía. • Coordinar la implantación de herramientas y controles de seguridad de la información y definir el		privacidad, integridad, disponibilidad, autenticidad y trazabilidad.

	cuadro de mando de la seguridad. Debe analizar y mantener actualizado dicho cuadro de mando.		
Responsables funcionales	• Definir la clasificación de la información • Determinar los niveles de acceso a la información • Autorizar la asignación de permisos de acceso • Apoyar al Área IT en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información	Dueños de la información (Directores y Managers)	Responsables de la información y su manejo
Área de tecnologías de la información y comunicaciones TICs	• Implantar en los SI los controles prescritos, acciones correctoras establecidas y gestionar las vulnerabilidades. • Cumplir con las normas y los procedimientos en materia de seguridad. Colaborar con el RSI en la definición de las mismas. • Requerir del RSI para el desarrollo/adaptación/implantación de nuevos productos del mercado que puedan tener un impacto importante. • Requerir participación del RSI en la gestión de cambio de hardware y software • Garantizar la inclusión de la seguridad en todo el ciclo de vida de la información y en los procesos de gestión de hardware y software. • Adoptar las medidas necesarias para proteger la información de acuerdo a las especificaciones de los dueños de la información. • Junto con el RSI identificar los riesgos y	Dpto. ICT e Infraestructura	Responsables de la implantación técnica, adopción de medidas y la gestión de las vulnerabilidades y cambios.

	propuestas de soluciones. Colaborar en las revisiones o auditorias de seguridad que se realizan.		
Personal de la empresa	• Mantener la confidencialidad de la información. • Hacer un buen uso de los equipos y de la información a la cual tienen acceso y protegerla de accesos no autorizados. • Respetar las normas y procedimientos vigentes en materia de seguridad de la información, y velar por que terceras partes en prestación de servicios también la respeten. • Utilizar adecuadamente las credenciales de acceso a los sistemas de información. • Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra que sea de aplicación. • Notificar, por la vía establecida, insuficiencias, anomalías o incidentes de seguridad y situaciones sospechosas que pudieran poner en peligro la seguridad de la información.	Toda persona que trabaja para la empresa (internos y externos)	Responsables por cumplimiento de las políticas en materia de seguridad de la información
Recursos Humanos	• Informar a las unidades gestoras de recursos de información sobre cambios movimientos de personal para poder realizar una buena gestión de recursos: altas, bajas definitivas y temporales, cambios de categoría y/o funciones, cambios organizativos, etc. • Trabajar conjuntamente con el RSI en el desarrollo de la política de seguridad de la	Director RRHH	Responsable de la gestión de recursos y de los procesos disciplinarios

	información en los temas referentes al personal. • Aplicar procedimientos disciplinarios en caso de vulneración del marco normativo.		
Otras Áreas	• Cada área dentro de la empresa deben colaborar con el RSI para dar los medios, definir, desplegar la seguridad en su campo de actuación con el objetivo conseguir trabajar y hacer trabajar la organización de manera segura dentro de los lineamientos de las política definidas.	Todas las departamentos, áreas dentro de la empresa	Responsables del trabajo en condiciones seguras.

ANEXO VIII

Metodología de análisis de Riesgos

1 Introducción

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.

El método que se aplica para el análisis de riesgos es el método Magerit v3 .

2 MAGERIT

El método implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones tomando en cuenta los riesgos derivados del uso de tecnologías de la información.

Objetivos de MAGERIT:

Directos:

1. concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

1. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Hay múltiples formas de tratar un riesgo. Evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, limitando sus consecuencias, compartirlo con otra organización (contratando un servicio o un seguro de cobertura), o en última instancia, aceptando que pudiera ocurrir y anticipando los recursos necesarios para actuar cuando sea necesario.

Proceso de Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo y comprende:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar las amenazas a las que están expuestos los activos.
3. Determinar de qué salvaguardas se disponen y cuán eficaces son ante al riesgo .

4. Estimar el impacto que es definido como el daño sobre el activo derivado de la materialización de la amenaza)
5. Estimar el riesgo que es definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

MAGERIT sigue un proceso para llegar a la identificacion de todos los riesgos de la organización.

Las fases de MAGERIT son las siguientes:

Fases de MAGERIT

Para este proyecto se sigue las distintas fases, las mismas que se detallan a continuación:

1. **Toma de datos y procesos de información**

   - Definir el alcance del análisis
   - Análisis de los procesos de la organización
   - Granularidad: unidades que se pretende analizar

2. **Dimensionamiento y establecimientos de parámetros**

   - Valoración económica de los activos (valor de reposición, valor de configuración, valor de uso y valor de perdida de oportunidad)

Valoración	Rango
Muy alta	Valor > 300000€
Alta	150000€<Valor > 300000€
Media	50000€<Valor > 150000€
Baja	10000€<Valor > 50000€

Muy baja	Valor < 10000 €

Valoración de activos

- Vulnerabilidad
  La frecuencia con la que puede una organización sufrir alguna amenaza en concreto. Esta frecuencia se la debe plasmar en una escala de valores.

Vulnerabilidad	Rango	Valor
Frecuencia extrema	Una vez al día	1
Frecuencia alta	Una vez cada dos semanas	26/365
Frecuencia media	Una vez cada 2 meses	6/365
Frecuencia baja	Una vez cada 6 meses	2/365
Frecuencia muy baja	Una vez al año	1/365

Tabla 2: Clasificación de las vulnerabilidad

- Impacto

  El tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente. Se definen los diferentes niveles de impacto que se utilizan y se asignan porcentajes de valor que se estima que se pierde en cada caso.

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

- Efectividad del control de seguridad

  Definir los niveles de influencia que tendrán las medidas de protección ante los riesgos que se van a detectar.

Variación Impacto/Vulnerabilidad	Valor
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

3. **Análisis de activos**

- Identificar los activos que posee y necesita para llevar a cabo sus actividades.

  - Activos físicos
  - Activos lógicos
  - Activos de personal
  - Activos e entorno e infraestructura
  - Activos intangibles

- Clasificar los activos según los valores establecidos

4. **Análisis de amenazas**

Amenazas son situaciones que pueden llegar a darse en una organización y que pueden desembocar en un problema de seguridad.

- Analizar las amenazas que afectaran los activos y englobarlos en alguno de los siguientes tipos de amenazas:
  - Accidentes
  - Errores
  - Amenazas intencionales presenciales
  - Amenazas intencionales remotas

5. **Establecimiento de vulnerabilidades**

Las vulnerabilidades son los agujeros que se tienen en la seguridad y que permitirán que una amenaza pueda dañar un activo

- Estimar la frecuencia de ocurrencia de una determinada amenaza sobre un activo

6. **Valoración del impacto**

Los impactos son las consecuencias que provoca en la organización el hecho de cierta amenaza afecte el activo.
Los impactos se analizan considerando:

- El resultado sobre el activo
- El efecto sobre cada activo para agrupar los impactos en cadena según la relación de activos
- El valor económico representativo de las perdidas producidas de cada activo

7. **Análisis de riesgo intrínseco**

Estudio de los riesgos actuales a los que la organización está sometida.

Riesgo = Valor activo x Vulnerabilidad x Impacto

8. **Influencia de salvaguardas**

Dos tipos fundamentales de controles de salvaguardas

- preventivas: reducen la vulnerabilidades
  Nueva vulnerabilidad = Vulnerabilidad x % de disminución de vulnerabilidad
- correctivas: reducen el impacto de las amenazas

Nuevo impacto = Impacto x Porcentaje de disminución de impacto

9. **Análisis de riesgos efectivos**
   Estudia cómo reducir los riesgos con cada una de las medidas de protección que se han identificado.
   - calcular el riesgo definitivo, riesgo efectivo que tendría la organización para cada una de las amenazas identificadas
10. **Gestión de Riesgos**
    - Toma de decisiones por parte de la organización sobre las medidas de seguridad a elegir de la lista de salvaguardas.
    - Escoger las medidas de seguridad que reduzcan los riesgos intrínsecos.
    - La gestión de riesgos incluye la elaboración de un plan de acción que contiene:
      - Establecimiento de prioridades
      - Planteamiento coste/beneficio
      - Selección de controles definitivos
      - Asignación de responsabilidades
      - Implantación de controles

ANEXO IX

Tabla de activos con sus valoraciones

SW

ID	Activo		Aspectos críticos				
		Valor	A	C	I	D	T
[SW.1]	Aplicación de gestión de datos clientes	MA	9	9	9	9	9
[SW.2]	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones	MA	8	8	8	9	9
[SW.3]	Aplicación de gestión de los datos personales de los empleados de la empresa	MA	8	8	8	9	8
[SW.4]	Aplicación de gestión de contratos de los clientes individuales	MA	8	8	8	8	8
[SW.5]	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas	MA	9	9	9	9	9
[SW.6]	Aplicación de gestión de contratos empresariales – seguros de grupo	MA	9	9	9	9	9
[SW.7]	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos	MA	8	8	8	9	8
[SW.8]	Aplicación contable de la empresa	MA	9	9	9	9	9
[SW.9]	Servidor de documentos de desarrollo	M	5	5	5	7	5
[SW.10]	Servidor de documentos en TST	M	7	7	7	7	7
[SW.11]	Servidor de documentos en INT	M	8	8	8	8	8
[SW.12]	Servidor de documentos en PRD	MA	9	9	9	9	9
[SW.13]	Servidor de aplicaciones de desarrollo	M	5	5	5	5	5
[SW.14]	Servidor de aplicaciones de test	M	6	6	6	6	6
[SW.15]	Servidor de aplicaciones de integración	A	7	7	7	7	7
[SW.16]	Servidor de aplicaciones de producción	MA	9	9	9	9	9
[SW.17]	SGBD Oracle en desarrollo	M	5	5	5	5	5
[SW.18]	SGBD Oracle en test	M	5	5	5	7	5
[SW.19]	SGBD Oracle en integración	A	7	8	8	7	8
[SW.20]	SGBD Oracle en producción	MA	9	9	9	9	9

HW							
ID	**Activo**		**Aspectos críticos**				
		Valor	**A**	**C**	**I**	**D**	**T**
[HW.1]	Servidor de aplicaciones internas/finanzas/admini/compta	MA	8	8	8	9	9
[HW.2]	Servidores DNS	MA	7	7	8	9	8
[HW.3]	Servidores DB Oracle prod	M	9	9	9	9	9
[HW.4]	Servidores DB Oracle dev	M	4	4	5	5	5
[HW.5]	Servidores DB Oracle test	A	5	5	5	7	7
[HW.6]	Servidores DB Oracle int	MA	9	8	8	9	8
[HW.7]	Servidores de e-comerce	MA				7	
[HW.8]	Routers	MA				8	
[HW.9]	Servidores de correo	M	8	8	8	8	7
[HW.10]	Servidores de Desarrollo	M	7	7	6	5	6
[HW.11]	Servidores de Test	A	7	8	8	7	8
[HW.12]	Servidores de Integración	A	9	9	9	9	9
[HW.13]	Servidores de Producción	MA	9	9	9	9	9
[HW.14]	PC Portables	M	7	7	7	8	7
[HW.15]	PC de escritorio fijas	M	6	7	7	5	7
[HW.16]	Tabletas	M				5	
[HW.17]	Teléfonos fijos	B				3	
[HW.18]	Teléfonos móviles	B				4	
[HW.19]	Dispositivos de conexión VPN	M				8	
[HW.20]	Rack de comunicaciones	MA				8	
[HW.21]	Switchs	MA				8	
[HW.22]	Firewalls	MA				7	
[HW.23]	Sistema Wifi	A				8	
[HW.24]	Cableado de la red	A				8	

[HW.25]	Cámaras de vigilancia	B				5	
[HW.26]	Servidor de documentos	MA				7	
[HW.27]	Servidores de copias de seguridad	MA				8	
[HW.28]	Multiservidores de impresión/scanner/fotocopias	B				5	
I							
			Aspectos críticos				
ID	**Activo**	Valor	A	C	I	D	T
[I.1]	Centro de procesamiento de datos	MA				9	
[I.2]	Salas de Reuniones	M				5	
[I.3]	Puestos de trabajo del personal – open spaces	A				8	
[I.4]	Puestos de trabajo bajo seguro	MA				7	
[I.5]	Oficinas de los directivos	MA				6	
[I.6]	Salas de impresión	M				4	
[I.7]	Unidades de apoyo a los servicios	M				4	
[I.8]	Espacios de almacenamiento de los racks	A				8	
[I.9]	Espacio de almacenamiento de documentos papel seguros	MA				8	
Datos							
			Aspectos críticos				
ID	**Activo**	Valor	A	C	I	D	T
[D.1]	Código fuentes aplicaciones de gestión de contratos	MA	9	10	10	10	9
[D.2]	Código fuente aplicaciones de gestión de usuarios	MA	9	10	10	10	9
[D.3]	Código fuente aplicaciones de gestión de datos de empleados	MA	9	10	10	10	9
[D.4]	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones	MA	9	10	10	10	9
[D.5]	Datos de clientes individuales	MA	9	10	9	9	8
[D.6]	Datos de clientes empresariales	MA	9	10	9	9	8

[D.7]	Datos de clientes independientes	MA	9	10	9	9	8
[D.8]	Datos de los empleados de la empresa	MA	8	10	9	7	8
[D.9]	Datos de acceso a las aplicaciones (roles y responsabilidades)	MA	8	9	8	9	9
[D.10]	Documentos de clientes	MA	8	8	8	9	8
[D.11]	Documentos de empleados	A	8	8	8	9	8
[D.12]	Documentos otros	M	5	6	7	7	8
[D.13]	Datos de soporte y licencias	M	5	6	7	7	8
[D.14]	Log de servidores y log de clientes	MA	9	10	10	10	9
[D.15]	Backup de DB usuarios	MA	8	8	9	9	9
[D.16]	Documentos en papel (contratos)	A	8	8	9	9	9
[D.17]	Backup código fuente	A	8	8	9	9	9
[D.18]	Backuo de DB Clientes	A	8	8	9	9	9
[D.19]	Backup DB empleados	A	8	8	9	9	9
[D.20]	Datos de configuración	A	8	8	9	9	9
COM							
			Aspectos críticos				
ID	**Activo**	Valor	A	C	I	D	T
[COM.1]	Internet	MA	8	8	8	8	7
[COM.2]	Red inalámbrica	A	8	8	8	7	7
[COM.3]	RED telefónica	M	6	5	5	7	5
[COM.4]	Cableado telecomunicaciones	MA	0	0	0	8	0
[COM.5]	Telefonía móvil	M	6	5	5	7	5
[COM.6]	Red Local	MA	8	8	8	9	8
[COM.7]	Cableado eléctrico	A	0	0	0	9	0
ID	Activo	Valor	A	C	I	D	T
[S.1]	Servicio Web	A	7	7	7	8	8

[S.2]	Servicio de aplicaciones	A				9	
[S.3]	Servicios de archivos	A	8	6	8	7	8
[S.4]	Servicios de documentos	A	8	6	8	7	8
[S.5]	Servicios DNS	A	7	8	8	8	7
[S.6]	Servicios email	M	7	7	8	6	6
[S.7]	Servicio comunicaciones	A	8	8	8	9	8
[S.8]	Portal interno	A	7	7	7	7	7
[S.9]	Portal Externo	A	9	8	8	9	9
AUX							
ID	**Activo**		**Aspectos críticos**				
		Valor	**A**	**C**	**I**	**D**	**T**
[AUX.1]	Lockers	M	0	0	0	6	0
[AUX.2]	Multiprinters	M	0	0	0	5	0
[AUX.3]	Recursos varios (material de escritorio, maletas, …)	B	0	0	0	3	0
[AUX.4]	Televisores	B	0	0	0	3	0
[AUX.5]	Equipos de sonido y proyección	B	0	0	0	3	0
[AUX.6]	Pantallas	B	0	0	0	3	0
[AUX.7]	Electricidad	A	0	0	0	8	0
[AUX.8]	Mobiliario	M	0	0	0	7	0
P							
ID	**Activo**		**Aspectos críticos**				
		Valor	**A**	**C**	**I**	**D**	**T**
[P.1]	Director General	MA	0	0	0	9	0
[P.2]	Director IT	A	0	0	0	8	0
[P.3]	Director operaciones	MA	0	0	0	9	0
[P.4]	Director de recursos humanos	M	0	0	0	4	0
[P.4]	Directos Riesgos	M	0	0	0	4	0
[P.5]	Director Finanzas	A	0	0	0	8	0

[P.6]	Director Marketing y ventas	M	0	0	0	3	0
[P.7]	Personal de desarrollo de las aplicaciones	A	0	0	0	6	0
[P.8]	Gestionarlos de contratos/Business Experto	MA	0	0	0	9	0
[P.9]	Personal RH	M	0	0	0	4	0
[P.10]	Administrador de la aplicación	A	0	0	0	7	0
[P.11]	Técnicos de soporte business	M	0	0	0	6	0
[P.12]	Agentes de ventas	M	0	0	0	4	0
[P.13]	Personal Comercial	M	0	0	0	4	0
[P.14]	Personal Finanzas	A	0	0	0	8	0
[P.15]	Personal Infraestructura	M	0	0	0	6	0
[P.16]	Personal Risks	M	0	0	0	4	0
[P.17]	Administradores de sistemas	A	0	0	0	6	0
[P.18]	Personal de soporte IT	M	0	0	0	5	0

ANEXO X

TABLA DE ANÁLISIS AMENAZAS/ACTIVOS

Grupo de Amenaza	Amenaza	Activo	Frecuencia/Amenaza		Impacto Amenaza				
			ID	Valor	A	C	I	D	T
[N] Desastres naturales									
	[N.1] Fuego								
		[HW] Hardware	MB	**0,002**				100%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				100%	
		[COM]: Redes	MB	**0,002**				100%	
		[I] Instalaciones	MB	**0,002**				100%	
		[P] Personal	MB	**0,002**				100%	
	[N.2] Daños por agua								
		[HW] Hardware	MB	**0,002**				75%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				75%	
		[COM]: Redes	MB	**0,002**				75%	
		[I] Instalaciones	MB	**0,002**				75%	
	[N.*] Desastres naturales								
		[SW] Software	MB	**0,002**				100%	
		[HW] Hardware	MB	**0,002**				100%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				100%	
		[I] Instalaciones	MB	**0,002**				100%	
[I] De origen industrial									
	[I.1] Fuego								
		[SW] Software	MB	**0,002**				100	

		[HW] Hardware	MB	**0,002**				100	
		[AUX] Equipo. Auxiliar	MB	**0,002**				100	
		[I] Instalaciones	MB	**0,002**				100	
	[I.2] Daños por agua								
		[SW] Software	MB	**0,002**				75%	
		[HW] Hardware	MB	**0,002**				75%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				75%	
		[I] Instalaciones	MB	**0,002**				75%	
	[I.*] Desastres industriales								
		[HW] Hardware	MB	**0,002**				75%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				20%	
		[I] Instalaciones	MB	**0,002**				75%	
	[I.3] Contaminación mecánica								
		[HW] Hardware	MB	**0,002**				50%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				50%	
		[I] Instalaciones	MB	**0,002**				50%	
	[I.4] Contaminación electromagnética								
		[HW] Hardware	MB	**0,002**				50%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				50%	
		[I] Instalaciones	MB	**0,002**				50%	
	[I.5] Avería de Origen Físico y lógico								
		[S] Servicios	B	**0,005**				50%	
		[SW] Software	B	**0,005**				50%	

		[HW] Hardware	B	**0,005**				50%	
		[AUX] Equip. Auxiliar	B	**0,005**				20%	
		[COM]: Redes	B	**0,005**				20%	
	[I.6] Corte de suministro eléctrico								
		[HW] Hardware	B	**0,005**				75%	
		[AUX] Equip. Auxiliar	B	**0,005**				50%	
	[I.7] Condiciones inadecuadas de temperatura o humedad								
		[HW] Hardware	B	**0,005**				50%	
		[AUX] Eqp. Auxiliar	B	**0,005**				20%	
		[COM]: Redes	B	**0,005**				20%	
	[I.8] Fallo de servicios de comunicaciones								
		[S] Servicios	M	**0,016**				100%	
		[SW] Software	M	**0,016**				100%	
		[HW] Hardware	M	**0,016**				100%	
		[AUX] Eqp. Auxiliar	M	**0,016**				100%	
		[COM]: Redes	M	**0,016**				20%	
		[AUX] Equipo. Auxiliar	B	**0,005**				20%	
		[HW] Hardware	MB	**0,002**				75%	
	[I.11] Emanaciones electromagnéticas								
		[HW] Hardware	MB	**0,002**		50%			
		[AUX] Equipo Auxiliar	MB	**0,002**		20%			
		[COM]: Redes	MB	**0,002**		20%			

		[I] Instalaciones	MB	**0,002**		20%			
[E] Errores y fallos no intencionados									
	[E.1] Errores de los usuarios								
		[D] Datos- Info	M	**0,016**		5%	5%	5%	
		[S] Servicios	M	**0,016**		5%	5%	5%	
		[SW] Software	M	**0,016**		5%	5%	5%	
	[E.2] Errores del administrador								
		[D] Datos- Info	M	**0,016**		20%	20%	20%	
		[S] Servicios	M	**0,016**		20%	20%	20%	
		[SW] Software	M	**0,016**		20%	20%	20%	
		[HW] Hardware	M	**0,016**		20%	20%	20%	
		[COM]: Redes	M	**0,016**		20%	20%	20%	
	[E.3] Errores de monitorización								
		[D] Datos- Info	M	**0,016**			50%		75%
	[E.4] Errores de configuración								
		[D] Datos- Info	M	**0,016**			50%		
	[E.7] Deficiencias en la organización								
		[P] Personal	M	**0,016**				75%	
	[E.8] Difusión de SW dañino								
		[SW] Software	MB	**0,002**		75%	50%	75%	
		[D] Datos- Info	MB	**0,002**		50%	50%	50%	
	[E.9] Errores de [re]-encaminamiento								
		[S] Servicios	MB	**0,002**		20%			
		[SW] Software	MB	**0,002**		50			

		[COM]: Redes	MB	**0,002**		50%			
	[E.10] Errores de secuencia								
		[S] Servicios	MB	**0,002**			20%		
		[SW] Software	MB	**0,002**			20%		
		[COM]: Redes	MB	**0,002**			20%		
	[E.15] Alteración accidental de la información								
		[D] Datos- Info	MB	**0,002**			50%		
		[S] Servicios	MB	**0,002**			5%		
		[SW] Software	MB	**0,002**			5%		
		[COM]: Redes	MB	**0,002**			5%		
		[I] Instalaciones	MB	**0,002**			5%		
	[E.18] Destrucción de la información								
		[D] Datos- Info	MB	**0,002**			100%		
		[S] Servicios	MB	**0,002**			75%		
		[SW] Software	MB	**0,002**			75%		
		[AUX] Equipo Auxiliar	MB	**0,002**			75%		
		[COM]: Redes	MB	**0,002**			20%		
		[I] Instalaciones	MB	**0,002**			5%		
	[E.19] Fugas de información								
		[D] Datos- Info	M	**0,016**		100%			
		[S] Servicios	M	**0,016**		50%			
		[SW] Software	M	**0,016**		50%			
		[COM]: Redes	M	**0,016**		50%			
		[I] Instalaciones	M	**0,016**		20%			
		[P] Personal	M	**0,016**		75%			

	[E.20] Vulnerabilidades de los programas (SW)								
		[SW] Software	MB	**0,002**		50%	50%	75%	
		[SW] Software	B	**0,005**			20%	75%	
		[HW] Hardware	B	**0,005**				75%	
		[AUX] Equipo Auxiliar	B	**0,005**				75%	
	[E.24] Caída del sistema por agotamiento de recursos								
		[S] Servicios	B	**0,005**				100%	
		[HW] Hardware	B	**0,005**				100%	
		[COM]: Redes	B	**0,005**				100%	
	[E.25] Perdida de equipos								
		[HW] Hardware	B	**0,005**		100%		100%	
	[E.28] Indisponibilidad del personal								
		[P] Personal	B	**0,005**				75%	
[A] Ataques intencionados									
	[A.3]Manipulación de los registros de actividad (log)								
		[D] Datos- Info	MB	**0,002**			75%		75%
	[A.4]Manipulación de la configuración								
		[D] Datos- Info	MB	**0,002**		50%	75%		75%
	[A.5]Suplantación de la identidad del usuario								
		[D] Datos- Info	B	**0,005**	100%	75%		50%	
		[S] Servicios	B	**0,005**	75%	75%		50%	

		[SW] Software	B	**0,005**	75%	75%		50%	
		[COM]: Redes	B	**0,005**	75%	75%		50%	
	[A.6]Abuso de privilegios de acceso								
		[D] Datos- Info	B	**0,005**		100%	50%	50%	
		[S] Servicios	B	**0,005**		75%			
		[SW] Software	B	**0,005**		75%	50%	50%	
		[HW] Hardware	B	**0,005**		75%	50%	50%	
		[COM]: Redes	B	**0,005**		75%	50%	50%	
	[A.7]Uso no previsto								
		[D] Datos- Info	MB	**0,002**		20%	20%	20%	
		[S] Servicios	MB	**0,002**		20%	20%	20%	
		[SW] Software	MB	**0,002**		20%	20%	20%	
		[HW] Hardware	MB	**0,002**		20%	20%	20%	
		[AUX] Equipo Auxiliar	MB	**0,002**		20%	20%	20%	
		[COM]: Redes	MB	**0,002**		20%	20%	20%	
		[I] Instalaciones	MB	**0,002**		20%	20%	20%	
	[A.8]Difusión de software dañino								
		[SW] Software	MB	**0,002**		75%	75%	75%	
	[A.9] [Re-]encaminamiento de mensajes								
		[S] Servicios	MB	**0,002**		50%			
		[SW] Software	MB	**0,002**		50%			
		[COM]: Redes	MB	**0,002**		50%			
	[A.10]Alteración de secuencia								
		[S] Servicios	MB	**0,002**			20%		
		[SW] Software	MB	**0,002**			20%		
		[COM]: Redes	MB	**0,002**			20%		
	[A.11]Acceso no								

	autorizado								
		[D] Datos- Info	M	**0,016**		100%	75%		
		[S] Servicios	M	**0,016**		50%	50%		
		[SW] Software	M	**0,016**		25%	25%		
		[HW] Hardware	M	**0,016**		50%	50%		
		[AUX] Equipo Auxiliar	M	**0,016**		20%	20%		
		[COM]: Redes	M	**0,016**		50%	50%		
		[I] Instalaciones	M	**0,016**		20%	20%		
	[A.12]Análisis de trafico								
		[COM]: Redes	B	**0,005**		100%			
	[A.13]Repudio								
		[D] Datos- Info	MB	**0,002**			50%		100%
		[S] Servicios	MB	**0,002**			50%		100%
	[A.14]Interceptación de información (escucha)								
		[COM]: Redes	MB	**0,002**		100%			
	[A.15]Modificación deliberada de la información								
		[D] Datos- Info	MB	**0,002**			100%		
		[S] Servicios	MB	**0,002**			20%		
		[SW] Software	MB	**0,002**			20%		
		[COM]: Redes	MB	**0,002**			20%		
		[I] Instalaciones	MB	**0,002**			20%		
	[A.18]Destrucción de información								
		[D] Datos- Info	MB	**0,002**				100%	
		[S] Servicios	MB	**0,002**				50%	
		[SW] Software	MB	**0,002**				20%	
		[I] Instalaciones	MB	**0,002**				20%	

	[A.19]Divulgación de información								
		[D] Datos- Info	B	**0,005**		75%			
		[S] Servicios	B	**0,005**		50%			
		[SW] Software	B	**0,005**		50%			
		[COM]: Redes	B	**0,005**		20%			
		[I] Instalaciones	B	**0,005**		20%			
	[A.22]Manipulación de programas								
		[SW] Software	MB	**0,002**		75%	50%	75%	
	[A.23]Manipulación de los equipos								
		[HW] Hardware	B	**0,005**		50%		50%	
		[AUX] Equipo Auxiliar	B	**0,005**		50%		50%	
	[A.24]Denegación de servicio								
		[S] Servicios	MB	**0,002**				100%	
		[HW] Hardware	MB	**0,002**				100%	
		[COM]: Redes	MB	**0,002**				100%	
	[A.25]Robo								
		[HW] Hardware				20%		100%	
		[AUX] Equipo Auxiliar				20%		100%	
	[A.26]Ataque destructivo								
		[HW] Hardware	B	**0,005**				100%	
		[AUX] Equipo Auxiliar	B	**0,005**				100%	
		[I] Instalaciones	B	**0,005**				100%	
	[A.27]Ocupación enemiga								
		[I] Instalaciones	MB	**0,002**		20%		100%	
	[A.28]Indisponibilidad del								

	personal								
		[P] Personal	A	**0,071**				100%	
	[A.29]Extorsión								
		[P] Personal	MB	**0,002**		20%	20%	20%	
	[A.30]Ingeniería social (picaresca)								
		[P] Personal	MB	**0,002**		20%	20%	20%	

ANEXO XI

VALORACION DEL IMPACTO POTENCIAL

ID	Activo	VALORACION					IMPACTO					IMPACTO POTENCIAL				
		A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
[SW.1]	Aplicación de gestión de datos clientes	9	9	9	9	9	75%	75%	75%	100%		6,75	6,75	6,75	9	0
[SW.2]	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones	8	8	8	9	9						6	6	6	9	0
[SW.3]	Aplicación de gestión de los datos personales de los empleados de la empresa	8	8	8	9	8						6	6	6	9	0
[SW.4]	Aplicación de gestión de contratos de los clientes individuales	8	8	8	8	8						6	6	6	8	0
[SW.5]	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas	9	9	9	9	9						6,75	6,75	6,75	9	0
[SW.6]	Aplicación de gestión de contratos empresariales – seguros de grupo	9	9	9	9	9						6,75	6,75	6,75	9	0
[SW.7]	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos	8	8	8	9	8						6	6	6	9	0
[SW.8]	Aplicación contable de la empresa	9	9	9	9	9						6,75	6,75	6,75	9	0
[SW.9]	Servidor de documentos de desarrollo	5	5	5	7	5						3,75	3,75	3,75	7	0
[SW.10]	Servidor de documentos en TST	7	7	7	7	7						5,25	5,25	5,25	7	0
[SW.11]	Servidor de documentos en INT	8	8	8	8	8						6	6	6	8	0
[SW.12]	Servidor de documentos en PRD	9	9	9	9	9						6,75	6,75	6,75	9	0
[SW.13]	Servidor de aplicaciones de desarrollo	5	5	5	5	5						3,75	3,75	3,75	5	0
[SW.14]	Servidor de aplicaciones de test	6	6	6	6	6						4,5	4,5	4,5	6	0

[SW.15]	Servidor de aplicaciones de integración	7	7	7	7	7						5,25	5,25	5,25	7	0
[SW.16]	Servidor de aplicaciones de producción	9	9	9	9	9						6,75	6,75	6,75	9	0
[SW.17]	SGBD Oracle en desarrollo	5	5	5	5	5						3,75	3,75	3,75	5	0
[SW.18]	SGBD Oracle en test	5	5	5	7	5						3,75	3,75	3,75	7	0
[SW.19]	SGBD Oracle en integración	7	8	8	7	8						5,25	6	6	7	0
[SW.20]	SGBD Oracle en producción	9	9	9	9	9						6,75	6,75	6,75	9	0
[HW.1]	Servidor de aplicaciones internas/finanzas/admini/compta	8	8	8	9	9		100%	50%	100%		0	8	4	9	0
[HW.2]	Servidores DNS	7	7	8	9	8						0	7	4	9	0
[HW.3]	Servidores DB Oracle prod	9	9	9	9	9						0	9	4,5	9	0
[HW.4]	Servidores DB Oracle dev	4	4	5	5	5						0	4	2,5	5	0
[HW.5]	Servidores DB Oracle test	5	5	5	7	7						0	5	2,5	7	0
[HW.6]	Servidores DB Oracle int	9	8	8	9	8						0	8	4	9	0
[HW.7]	Servidores de e-comerce				7							0	0	0	7	0
[HW.8]	Routers				8							0	0	0	8	0
[HW.9]	Servidores de correo	8	8	8	8	7						0	0	0	8	0
[HW.10]	Servidores de Desarrollo	7	7	6	5	6						0	0	0	5	0
[HW.11]	Servidores de Test	7	8	8	7	8						0	0	0	7	0
[HW.12]	Servidores de Integración	9	9	9	9	9						0	0	0	9	0

[HW.13]	Servidores de Producción	9	9	9	9	9						0	0	0	9	0
[HW.14]	PC Portables	7	7	7	8	7						0	0	0	8	0
[HW.15]	PC de escritorio fijas	6	7	7	5	7						0	0	0	5	0
[HW.16]	Tabletas				5							0	0	0	5	0
[HW.17]	Teléfonos fijos				3							0	0	0	3	0
[HW.18]	Teléfonos móviles				4							0	0	0	4	0
[HW.19]	Dispositivos de conexión VPN				8							0	0	0	8	0
[HW.20]	Rack de comunicaciones				8							0	0	0	8	0
[HW.21]	Switchs				8							0	0	0	8	0
[HW.22]	Firewalls				7							0	0	0	7	0
[HW.23]	Sistema Wifi				8							0	0	0	8	0
[HW.24]	Cableado de la red				8							0	0	0	8	0
[HW.25]	Cámaras de vigilancia				5							0	0	0	5	0
[HW.26]	Servidor de documentos	7	8	8	8	7						0	8	4	8	0
[HW.27]	Servidor de copias de seguridad	8	7	8	9	7						0	7	4	9	0
[HW.28]	Multiservidores de impresión/scanner/fotocopias				5							0	0	0	5	0
[I.1]	Centro de procesamiento de datos				9			20%	20%	100%		0	0	0	9	0
[I.2]	Salas de Reuniones				5							0	0	0	5	0
[I.3]	Puestos de trabajo del personal – open spaces				8							0	0	0	8	0

[I.4]	Puestos de trabajo bajo seguro				7							0	0	0	7	0
[I.5]	Oficinas de los directivos				6							0	0	0	6	0
[I.6]	Salas de impresión				4							0	0	0	4	0
[I.7]	Unidades de apoyo a los servicios				4							0	0	0	4	0
[I.8]	Espacios de almacenamiento de los racks				8							0	0	0	8	0
[I.9]	Espacio de almacenamiento de documentos papel seguros				8							0	0	0	8	0
[D.1]	Código fuentes aplicaciones de gestión de contratos	9	10	10	10	9	100%	100%	100 %	100%	100%	9	10	10	10	9
[D.2]	Código fuente aplicaciones de gestión de usuarios	9	10	10	10	9						9	10	10	10	9
[D.3]	Código fuente aplicaciones de gestión de datos de empleados	9	10	10	10	9						9	10	10	10	9
[D.4]	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones	9	10	10	10	9						9	10	10	10	9
[D.5]	Datos de clientes individuales	9	10	9	9	8						9	10	9	9	8
[D.6]	Datos de clientes empresariales	9	10	9	9	8						9	10	9	9	8
[D.7]	Datos de clientes independientes	9	10	9	9	8						9	10	9	9	8
[D.8]	Datos de los empleados de la empresa	8	10	9	7	8						8	10	9	7	8
[D.9]	Datos de acceso a las aplicaciones (roles y responsabilidades)	8	9	8	9	9						8	9	8	9	9
[D.10]	Documentos de clientes	8	8	8	9	8						8	8	8	9	8
[D.11]	Documentos de empleados	8	8	8	9	8						8	8	8	9	8
[D.12]	Documentos otros	5	6	7	7	8						5	6	7	7	8

[D.13]	Datos de soporte y licencias	5	6	7	7	8						5	6	7	7	8
[D.14]	Log de servidores y log de clientes	9	10	10	10	9						9	10	10	10	9
[D.15]	Backus de DB users	8	8	9	9	9						8	8	9	9	9
[D.16]	Documentos en papel (contratos)	8	8	9	9	9						8	8	9	9	9
[D.17]	Backup código fuente	8	8	9	9	9						8	8	9	9	9
[D.18]	Backuo de DB Clientes	8	8	9	9	9						8	8	9	9	9
[D.19]	Backup DB empleados	8	8	9	9	9						8	8	9	9	9
[D.20]	Datos de configuración	8	8	9	9	9						8	8	9	9	9
[COM.1]	Internet	8	8	8	8	7		100%	50%	100%		0	8	4	8	0
[COM.2]	Red inalámbrica	8	8	8	7	7						0	8	4	7	0
[COM.3]	RED telefónica	6	5	5	7	5						0	5	2,5	7	0
[COM.4]	Cableado telecomunicaciones	0	0	0	8	0						0	0	0	8	0
[COM.5]	Telefonía móvil	6	5	5	7	5						0	0	0	7	0
[COM.6]	Red Local	8	8	8	9	8							8	4	9	0
[COM.7]	Cableado eléctrico	0	0	0	9	0						0	0	0	0	0
[S.1]	Servicio Web	7	7	7	8	8	75%	75%	75%	100%	100%	5,25	5,25	5,25	8	8
[S.2]	Servicio de aplicaciones				9							0	0	0	9	0
[S.3]	Servicios de archivos	8	6	8	7	8						6	4,5	6	7	8
[S.4]	Servicios de documentos	8	6	8	7	8						6	4,5	6	7	8

[S.5]	Servicios DNS	7	8	8	8	7						5,25	6	6	8	7
[S.6]	Servicios email	7	7	8	6	6						5,25	5,25	6	6	6
[S.7]	Servicio comunicaciones	8	8	8	9	8						6	6	6	9	8
[S.8]	Portal interno	7	7	7	7	7						5,25	5,25	5,25	7	7
[S.9]	Portal Externo	9	8	8	9	9						6,75	6	6	9	9
[AUX.1]	Lockers	0	0	0	6	0		50%	75%	100%		0	0	0	6	0
[AUX.2]	Multiprinters	0	0	0	5	0						0	0	0	5	0
[AUX.3]	Recursos varios (material de escritorio, maletas,	0	0	0	3	0						0	0	0	3	0
[AUX.4]	Televisores	0	0	0	3	0						0	0	0	3	0
[AUX.5]	Equipos de sonido y proyección	0	0	0	3	0						0	0	0	3	0
[AUX.6]	Pantallas	0	0	0	3	0						0	0	0	3	0
[AUX.7]	Electricidad	0	0	0	8	0						0	0	0	8	0
[AUX.8]	Mobiliario	0	0	0	7	0						0	0	0	7	0
[P.1]	Director General	0	0	0	9	0		75%	20%	100%		0	0	0	9	0
[P.2]	Director IT	0	0	0	8	0						0	0	0	8	0
[P.3]	Director operaciones	0	0	0	9	0						0	0	0	9	0
[P.4]	Director de recursos humanos	0	0	0	4	0						0	0	0	4	0
[P.4]	Directos Riesgos	0	0	0	4	0						0	0	0	4	0

[P.5]	Director Finanzas	0	0	0	7	0						0	0	0	7	0	
[P.6]	Director Marketing y ventas	0	0	0	4	0						0	0	0	4	0	
[P.7]	Personal de desarrollo de las aplicaciones	0	0	0	7	0						0	0	0	7	0	
[P.8]	Gestionaros de contratos/Business Experto	0	0	0	9	0						0	0	0	9	0	
[P.9]	Personal RH	0	0	0	4	0						0	0	0	4	0	
[P.10]	Administrador de la aplicación	0	0	0	8	0						0	0	0	8	0	
[P.11]	Técnicos de soporte budines	0	0	0	7	0						0	0	0	7	0	
[P.12]	Agentes de ventas	0	0	0	5	0						0	0	0	5	0	
[P.13]	Personal Comercial	0	0	0	5	0						0	0	0	5	0	
[P.14]	Personal Fínanse	0	0	0	8	0						0	0	0	8	0	
[P.15]	Personal Infraestructura	0	0	0	7	0						0	0	0	7	0	
[P.16]	Personal Risks	0	0	0	5	0						0	0	0	5	0	
[P.17]	Administradores de sistemas	0	0	0	7	0						0	0	0	7	0	
[P.18]	Personal de soporte IT	0	0	0	5	0						0	0	0	5	0	

ANEXO XII

TABLA DE VALORACION DE RIESGO

Tipo	Activo	Valor	Freq.	IMPACTO POTENCIAL					RIESGO				
				A	C	I	D	T	A	C	I	D	T
[SW.1]	Aplicación de gestión de datos clientes	M	0,016	6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0
[SW.2]	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones			6	6	6	9	0	0,10	0,10	0,10	0,14	0
[SW.3]	Aplicación de gestión de los datos personales de los empleados de la empresa			6	6	6	9	0	0,10	0,10	0,10	0,14	0
[SW.4]	Aplicación de gestión de contratos de los clientes individuales			6	6	6	8	0	0,10	0,10	0,10	0,13	0
[SW.5]	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas			6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0
[SW.6]	Aplicación de gestión de contratos empresariales – seguros de grupo			6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0
[SW.7]	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos			6	6	6	9	0	0,10	0,10	0,10	0,14	0
[SW.8]	Aplicación contable de la empresa			6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0
[SW.9]	Servidor de documentos de desarrollo			3,75	3,75	3,75	7	0	0,06	0,06	0,06	0,11	0
[SW.10]	Servidor de documentos en TST			5,25	5,25	5,25	7	0	0,08	0,08	0,08	0,11	0
[SW.11]	Servidor de documentos en INT			6	6	6	8	0	0,10	0,10	0,10	0,13	0
[SW.12]	Servidor de documentos en PRD			6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0
[SW.13]	Servidor de aplicaciones de desarrollo			3,75	3,75	3,75	5	0	0,06	0,06	0,06	0,08	0
[SW.14]	Servidor de aplicaciones de test			4,5	4,5	4,5	6	0	0,07	0,07	0,07	0,10	0
[SW.15]	Servidor de aplicaciones de integración			5,25	5,25	5,25	7	0	0,08	0,08	0,08	0,11	0
[SW.16]	Servidor de aplicaciones de producción			6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0
[SW.17]	SGBD Oracle en desarrollo			3,75	3,75	3,75	5	0	0,06	0,06	0,06	0,08	0
[SW.18]	SGBD Oracle en test			3,75	3,75	3,75	7	0	0,06	0,06	0,06	0,11	0
[SW.19]	SGBD Oracle en integración			5,25	6	6	7	0	0,08	0,10	0,10	0,11	0
[SW.20]	SGBD Oracle en producción			6,75	6,75	6,75	9	0	0,11	0,11	0,11	0,14	0

[HW.1]	Servidor de aplicaciones internas/finanzas/admini/compta	M	0,016	0	8	4	9	0	0	0,13	0,06	0,14	0
[HW.2]	Servidores DNS			0	7	4	9	0	0	0,11	0,06	0,14	0
[HW.3]	Servidores DB Oracle prod			0	9	4,5	9	0	0	0,14	0,07	0,14	0
[HW.4]	Servidores DB Oracle dev			0	4	2,5	5	0	0	0,06	0,04	0,08	0
[HW.5]	Servidores DB Oracle test			0	5	2,5	7	0	0	0,08	0,04	0,11	0
[HW.6]	Servidores DB Oracle int			0	8	4	9	0	0	0,13	0,06	0,14	0
[HW.7]	Servidores de e-comerce			0	0	0	7	0	0	0	0	0,11	0
[HW.8]	Routers			0	0	0	8	0	0	0	0	0,13	0
[HW.9]	Servidores de correo			0	0	0	8	0	0	0	0	0,13	0
[HW.10]	Servidores de Desarrollo			0	0	0	5	0	0	0	0	0,08	0
[HW.11]	Servidores de Test			0	0	0	7	0	0	0	0	0,11	0
[HW.12]	Servidores de Integración			0	0	0	9	0	0	0	0	0,14	0
[HW.13]	Servidores de Producción			0	0	0	9	0	0	0	0	0,14	0
[HW.14]	PC Portables			0	0	0	8	0	0	0	0	0,13	0
[HW.15]	PC de escritorio fijas			0	0	0	5	0	0	0	0	0,08	0
[HW.16]	Tabletas			0	0	0	5	0	0	0	0	0,08	0
[HW.17]	Teléfonos fijos			0	0	0	3	0	0	0	0	0,05	0
[HW.18]	Teléfonos móviles			0	0	0	4	0	0	0	0	0,06	0
[HW.19]	Dispositivos de conexión VPN			0	0	0	8	0	0	0	0	0,13	0
[HW.20]	Rack de comunicaciones			0	0	0	8	0	0	0	0	0,13	0
[HW.21]	Switchs			0	0	0	8	0	0	0	0	0,13	0
[HW.22]	Firewalls			0	0	0	7	0	0	0	0	0,11	0
[HW.23]	Sistema Wifi			0	0	0	8	0	0	0	0	0,13	0
[HW.24]	Cableado de la red			0	0	0	8	0	0	0	0	0,13	0
[HW.25]	Cámaras de vigilancia			0	0	0	5	0	0	0	0	0,08	0
[HW.26]	Servidor de documentos			0	8	4	8	0	0	0,13	0,06	0,13	0
[HW.27]	Servidor de copias de seguridad			0	7	4	9	0	0	0,11	0,06	0,14	0
[HW.28]	Multiservidores de impresión/scanner/fotocopias			0	0	0	5	0	0	0	0	0,08	0
[I.1]	Centro de procesamiento de datos	M	0,016	0	0	0	9	0	0	0	0	0,14	0

[I.2]	Salas de Reuniones			0	0	0	5	0	0	0	0	0,08	0
[I.3]	Puestos de trabajo del personal – open spaces			0	0	0	8	0	0	0	0	0,13	0
[I.4]	Puestos de trabajo bajo seguro			0	0	0	7	0	0	0	0	0,11	0
[I.5]	Oficinas de los directivos			0	0	0	6	0	0	0	0	0,10	0
[I.6]	Salas de impresión			0	0	0	4	0	0	0	0	0,06	0
[I.7]	Unidades de apoyo a los servicios			0	0	0	4	0	0	0	0	0,06	0
[I.8]	Espacios de almacenamiento de los racks			0	0	0	8	0	0	0	0	0,13	0
[I.9]	Espacio de almacenamiento de documentos papel seguros			0	0	0	8	0	0	0	0	0,13	0
[D.1]	Código fuentes aplicaciones de gestión de contratos	M	0,016	9	10	10	10	9	0,14	0,16	0,16	0,16	0,14
[D.2]	Código fuente aplicaciones de gestión de usuarios			9	10	10	10	9	0,14	0,16	0,16	0,16	0,14
[D.3]	Código fuente aplicaciones de gestión de datos de empleados			9	10	10	10	9	0,14	0,16	0,16	0,16	0,14
[D.4]	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones			9	10	10	10	9	0,14	0,16	0,16	0,16	0,14
[D.5]	Datos de clientes individuales			9	10	9	9	8	0,14	0,16	0,14	0,14	0,13
[D.6]	Datos de clientes empresariales			9	10	9	9	8	0,14	0,16	0,14	0,14	0,13
[D.7]	Datos de clientes independientes			9	10	9	9	8	0,14	0,16	0,14	0,14	0,13
[D.8]	Datos de los empleados de la empresa			8	10	9	7	8	0,13	0,16	0,14	0,11	0,13
[D.9]	Datos de acceso a las aplicaciones (roles y responsabilidades)			8	9	8	9	9	0,13	0,14	0,13	0,14	0,14
[D.10]	Documentos de clientes			8	8	8	9	8	0,13	0,13	0,13	0,14	0,13
[D.11]	Documentos de empleados			8	8	8	9	8	0,13	0,13	0,13	0,14	0,13
[D.12]	Documentos otros			5	6	7	7	8	0,08	0,10	0,11	0,11	0,13
[D.13]	Datos de soporte y licencias			5	6	7	7	8	0,08	0,10	0,11	0,11	0,13
[D.14]	Log de servidores y log de clientes			9	10	10	10	9	0,14	0,16	0,16	0,16	0,14
[D.15]	Backup de DB users			8	8	9	9	9	0,13	0,13	0,14	0,14	0,14
[D.16]	Documentos en papel (contratos)			8	8	9	9	9	0,13	0,13	0,14	0,14	0,14
[D.17]	Backup código fuente			8	8	9	9	9	0,13	0,13	0,14	0,14	0,14
[D.18]	Backuo de DB Clientes			8	8	9	9	9	0,13	0,13	0,14	0,14	0,14
[D.19]	Backup DB empleados			8	8	9	9	9	0,13	0,13	0,14	0,14	0,14
[D.20]	Datos de configuración			8	8	9	9	9	0,13	0,13	0,14	0,14	0,14

[COM.1]	Internet	M	0,016	0	8	4	8	0	0	0,13	0,06	0,13	0
[COM.2]	Red inalámbrica			0	8	4	7	0	0	0,13	0,06	0,11	0
[COM.3]	RED telefónica			0	5	2,5	7	0	0	0,08	0,04	0,11	0
[COM.4]	Cableado telecomunicaciones			0	0	0	8	0	0	0	0,00	0,13	0
[COM.5]	Telefonía móvil			0	0	0	7	0	0	0	0,00	0,11	0
[COM.6]	Red Local				8	4	9	0	0	0,13	0,06	0,14	0
[COM.7]	Cableado eléctrico			0	0	0	8	0	0	0	0,00	0,13	0
[S.1]	Servicio Web	M	0,016	5,25	5,25	5,25	8	8	0,08	0,08	0,08	0,13	0,13
[S.2]	Servicio de aplicaciones			0	0	0	9	0	0	0	0	0,14	0
[S.3]	Servicios de archivos			6	4,5	6	7	8	0,10	0,07	0,10	0,11	0,13
[S.4]	Servicios de documentos			6	4,5	6	7	8	0,10	0,07	0,10	0,11	0,13
[S.5]	Servicios DNS			5,25	6	6	8	7	0,08	0,10	0,10	0,13	0,11
[S.6]	Servicios email			5,25	5,25	6	6	6	0,08	0,08	0,10	0,10	0,10
[S.7]	Servicio comunicaciones			6	6	6	9	8	0,10	0,10	0,10	0,14	0,13
[S.8]	Portal interno			5,25	5,25	5,25	7	7	0,08	0,08	0,08	0,11	0,11
[S.9]	Portal Externo			6,75	6	6	9	9	0,11	0,10	0,10	0,14	0,14
[AUX.1]	Lockers	M	0,016	0	0	0	6	0	0	0	0	0,10	0
[AUX.2]	Multiprinters			0	0	0	5	0	0	0	0	0,08	0
[AUX.3]	Recursos varios (material de escritorio, maletas, …)			0	0	0	3	0	0	0	0	0,05	0
[AUX.4]	Televisores			0	0	0	3	0	0	0	0	0,05	0
[AUX.5]	Equipos de sonido y proyección			0	0	0	3	0	0	0	0	0,05	0
[AUX.6]	Pantallas			0	0	0	3	0	0	0	0	0,05	0
[AUX.7]	Cableado eléctrico			0	0	0	8	0	0	0	0	0,13	0
[AUX.8]	Mobiliario			0	0	0	5	0	0	0	0	0,08	0
[P.1]	Director General	A	0,071	0	0	0	9	0	0	0	0	0,64	0
[P.2]	Director IT			0	0	0	8	0	0	0	0	0,57	0
[P.3]	Director operaciones			0	0	0	9	0	0	0	0	0,64	0
[P.4]	Director de recursos humanos			0	0	0	4	0	0	0	0	0,28	0
[P.4]	Director Riesgos			0	0	0	4	0	0	0	0	0,28	0

[P.5]	Director Finanzas			0	0	0	7	0	0	0	0	0,50	0
[P.6]	Director Marketing y ventas			0	0	0	4	0	0	0	0	0,28	0
[P.7]	Personal de desarrollo de las aplicaciones			0	0	0	7	0	0	0	0	0,50	0
[P.8]	Gestionaros de contratos/Business Experto			0	0	0	9	0	0	0	0	0,64	0
[P.9]	Personal RH			0	0	0	4	0	0	0	0	0,28	0
[P.10]	Administrador de la aplicación			0	0	0	8	0	0	0	0	0,57	0
[P.11]	Técnicos de soporte buSiness			0	0	0	7	0	0	0	0	0,50	0
[P.12]	Agentes de ventas			0	0	0	5	0	0	0	0	0,36	0
[P.13]	Personal Comercial			0	0	0	5	0	0	0	0	0,36	0
[P.14]	Personal Fínanzas			0	0	0	8	0	0	0	0	0,57	0
[P.15]	Personal Infraestructura			0	0	0	7	0	0	0	0	0,50	0
[P.16]	Personal Risks			0	0	0	5	0	0	0	0	0,36	0
[P.17]	Administradores de sistemas			0	0	0	7	0	0	0	0	0,50	0
[P.18]	Personal de soporte IT			0	0	0	5	0	0	0	0	0,36	0

ANEXO XIII

Grupos de Amenazas

Grupo	Amenaza
[N] Desastres naturales	
	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
[I] De origen industrial	
	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación mecánica
	[I.4] Contaminación electromagnética
	[I.5] Avería de Origen Físico y lógico
	[I.6] Corte de suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	
	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.3] Errores de monitorización
	[E.4] Errores de configuración
	[E.7] Deficiencias en la organización
	[E.8] Difusión de SW dañino
	[E.9] Errores de [re]-encaminamiento
	[E.10] Errores de secuencia
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (SW)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Perdida de equipos
	[E.28] Indisponibilidad del personal
[A] Ataques intencionados	
	[A.3]Manipulación de los registros de actividad (log)
	[A.4]Manipulación de la configuración
	[A.5]Suplantación de la identidad del usuario
	[A.6]Abuso de privilegios de acceso

	[A.7]Uso no previsto
	[A.8]Difusión de software dañino
	[A.9] [Re-]encaminamiento de mensajes
	[A.10]Alteración de secuencia
	[A.11]Acceso no autorizado
	[A.12]Análisis de trafico
	[A.13]Repudio
	[A.14]Interceptación de información (escucha)
	[A.15]Modificación deliberada de la información
	[A.18]Destrucción de información
	[A.19]Divulgación de información
	[A.22]Manipulación de programas
	[A.23]Manipulación de los equipos
	[A.24]Denegación de servicio
	[A.25]Robo
	[A.26]Ataque destructivo
	[A.27]Ocupación enemiga
	[A.28]Indisponibilidad del personal
	[A.29]Extorsión
	[A.30]Ingeniería social (picaresca)

ANEXO XIV

Nivel de cumplimiento de la norma ISO/IEC 27002:2013 después de la implantación de los proyectos.

Control	% implementación		Proyecto
	Actual	Después	
5 POLÍTICAS DE SEGURIDAD	50%	100%	Políticas de la seguridad de la Información
5.1 Directrices de la Dirección en seguridad de la información	50%	100%	
5.1.1 Conjunto de políticas para la seguridad de la información	60%	100%	
5.1.2 Revisión de las políticas para la seguridad de la información	40%	100%	
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	46%	56%	
6.1 Organización interna	49%	62%	
6.1.1 Asignación de responsabilidades para la seguridad de la información	60%	80%	Políticas de la seguridad de la información
6.1.2 Segregación de tareas	60%	60%	
6.1.3 Contacto con las autoridades	70%	70%	
6.1.4 Contacto con grupos de interés especial	70%	70%	
6.1.5 Seguridad de la información en la gestión de proyectos	30%	30%	
6.2 Dispositivos para movilidad y teletrabajo	43%	50%	
6.2.1 Política de uso de dispositivos para movilidad	40%	50%	
6.2.2 Teletrabajo	45%	50%	
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	57%	100%	
7.1 Antes de la contratación	60%	100%	Gestión del personal
7.1.1 Investigación de antecedentes	60%	100%	Gestión del personal
7.1.2 Términos y condiciones de contratación	60%	100%	
7.2 Durante la contratación	60%	100%	

7.2.1 Responsabilidades de gestión	60%	100%	Gestión del personal
7.2.2 Concienciación, educación y capacitación en seguridad de la información	60%	100%	Proceso de formación continua
7.2.3 Proceso disciplinario	60%	100%	Gestión del personal
7.3 Cese o cambio de puesto de trabajo	50%	100%	Gestión del personal
7.3.1 Cese o cambio de puesto de trabajo	50%	100%	
8. GESTIÓN DE ACTIVOS	61%	75%	
8.1 Responsabilidad sobre los activos	70%	83%	
8.1.1 Inventario de activos	80%	80%	
8.1.2 Propiedad de los activos	70%	90%	Mejora en la gestión de recursos humanos
8.1.3 Uso aceptable de los activos	60%	80%	Políticas de la información/Mejora en la gestión de RH
8.1.4 Devolución de activos	70%	80%	Mejora en la Gestión de RH
8.2 Clasificación de la información	70%	100%	
8.2.1 Directrices de clasificación	70%	100%	Clasificación de la información
8.2.2 Etiquetado y manipulado de la información	70%	100%	Clasificación de la información
8.2.3 Manipulación de activos	70%	100%	Clasificación de la información
8.3 Manejo de los soportes de almacenamiento	42%	42%	
8.3.1 Gestión de soportes extraíbles	40%	40%	
8.3.2 Eliminación de soportes	45%	45%	
8.3.3 Soportes físicos en tránsito	40%	40%	
9. CONTROL DE ACCESOS	65%	100%	
9.1 Requisitos de negocio para el control de accesos	70%	100%	Política de control de acceso/ 2F autenticación
9.1.1 Política de control de accesos	80%	100%	
9.1.2 Control de acceso a las redes y servicios asociados	60%	100%	2F autenticación
9.2 Gestión de acceso de usuario	58%	100%	

9.2.1 Registro de acceso y baja de usuarios	70%	100%	Gestión de acceso del usuario
9.2.2 Provisión de acceso de usuario	60%	100%	
9.2.3 Gestión de privilegios de acceso	60%	100%	
9.2.4 Gestión de la información secreta de autenticación de los usuarios	50%	100%	
9.2.5 Revisión de los derechos de acceso del usuario	55%	100%	
9.2.6 Retirada o reasignación de los derechos de acceso	55%	100%	Gestión de Personal
9.3 Responsabilidades del usuario	65%	100%	
9.3.1 Uso de la información secreta de la autenticación	65%	100%	Proceso de gestión de personal
9.4 Control de acceso a sistemas y aplicaciones	68%	98%	Control de acceso al sistema y aplicaciones
9.4.1 Restricción de acceso a la información	80%	100%	
9.4.2 Procedimientos seguros de inicio de sesión	60%	100%	
9.4.3 Sistema de gestión de contraseñas	70%	100%	
9.4.4 Uso de utilidades con privilegios del sistema	70%	90%	
9.4.5 Control de acceso al código fuente de los programas	60%	100%	
10. CRIPTOGRAFIA	65%	65%	
10.1 Controles criptográficos	65%	65%	
10.1.1 Política de uso de los controles criptográficos	60%	60%	
10.1.2 Gestión de claves	70%	70%	
11. SEGURIDAD FISICA DEL ENTORNO	72%	72%	
11.1 Áreas seguras	78%	78%	
11.1.1 Perímetro de seguridad física	80%	80%	
11.1.2 Controles físicos de entrada	90%	90%	
11.1.3 Seguridad de oficinas, despachos y recursos	70%	70%	
11.1.4 Protección contra las amenazas externas y ambientales	80%	80%	
11.1.5 El trabajo en áreas seguras	80%	80%	

11.1.6 Áreas de carga y descarga	70%	70%	
11.2 Seguridad de los equipos	66%	66%	
11.2.1 Emplazamiento y protección de equipos	65%	65%	
11.2.2 Instalaciones de suministro	80%	80%	
11.2.3 Seguridad del cableado	80%	80%	
11.2.4 Mantenimiento de los equipos	80%	80%	
11.2.5 Retirada de materiales propiedad de la empresa	60%	60%	
11.2.6 Seguridad de los equipos fuera de las instalaciones	60%	60%	
11.2.7 Reutilización o eliminación segura de equipos	60%	60%	
11.2.8 Equipo de usuario desatendido	60%	60%	
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	50%	50%	
12. SEGURIDAD DE LAS OPERACIONES	68%	81%	
12.1 Procedimientos y responsabilidades operacionales	55%	55%	
12.1.1 Documentación de procedimientos de las operaciones	70%	70%	
12.1.2 Gestión de cambios	50%	50%	
12.1.3 Gestión de capacidades	50%	50%	
12.1.4 Separación de los recursos de desarrollo, prueba y operaciones	50%	50%	
12.2 Protección contra el software malicioso	70%	70%	
12.2.1 Controles contra el código malicioso	70%	70%	
12.3 Copias de seguridad	70%	100%	Copias de Respaldo
12.3.1 Copias de seguridad de la información	70%	100%	
12.4 Registros y supervisión	63%	63%	
12.4.1 Registro de eventos	70%	70%	
12.4.2 Protección de la información de registro	60%	60%	
12.4.3 Registros de administración y operación	70%	70%	

12.4.4 Sincronización del reloj	50%	50%	
12.5 Control del software en explotación	60%	60%	
12.5.1 Instalación del software en explotación	60%	60%	
12.6 Gestión de la vulnerabilidad técnica	50%	50%	
12.6.1 Gestión de la vulnerabilidad técnica	50%	50%	
12.6.2 Restricción en la instalación del software	50%	50%	
12.7 Consideraciones sobre la auditoria de sistemas de información	40%	90%	
12.7.1 Controles de auditoria de sistemas de información	40%	90%	Control de acceso al sistema y aplicaciones
13. Seguridad de las comunicaciones	58%	60%	
13.1 Gestión de la seguridad de redes	47%	47%	
13.1.1 Controles de red	50%	50%	
13.1.2 Seguridad de los servicios de red	50%	50%	
13.1.3 Segregación en redes	40%	40%	
13.2 Intercambio de información	70%	73%	
13.2.1 Políticas y procedimientos en intercambio de información	60%	60%	
13.2.2 Acuerdos de intercambio de información	70%	70%	
13.2.3 Mensajería electrónica	70%	70%	
13.2.4 Acuerdos de confidencialidad o no revelación	80%	90%	Mejora en la gestión de RH
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	65%	66%	
14.1 Requisitos de seguridad en sistemas de información	70%	73%	
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	60%	60%	
14.1.2 Asegurar los servicios de aplicaciones en redes publicas	70%	80%	
14.1.3 Protecciones de las transacciones de servicios de aplicaciones	80%	80%	
14.2 Seguridad en el desarrollo y en los procesos de soporte	56%	56%	

14.2.1 Política de desarrollo seguro	50%	50%	
14.2.2 Procedimiento de control de cambios en el sistema	50%	50%	
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	70%	70%	
14.2.4 Restricciones a los cambios en los paquetes de software	50%	50%	
14.2.5 Principios de ingeniería de sistemas seguros	50%	50%	
14.2.6 Entorno de desarrollo seguro	50%	50%	
14.2.7 Externalización del desarrollo de software	50%	50%	
14.2.8 Pruebas funcionales de seguridad del sistema	70%	70%	
14.2.9 pruebas de aceptación del sistema	65%	65%	
14.3 Datos de prueba	70%	70%	
14.3.1 Protección de los datos de prueba	70%	70%	
15. RELACIONES CON PROVEEDORES	64%	64%	
15.1 Seguridad en las relaciones con los proveedores	73%	73%	
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	70%	70%	
15.1.2 Requisitos de seguridad en contratos con terceros	75%	75%	
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	75%	75%	
15.2 gestión de la provisión de los servicios del proveedor	55%	55%	
15.2.1 Control y revisión de la provisión de servicios del proveedor	55%	55%	
15.2.2 Gestión de cambios en la provisiones del proveedor	55%	55%	
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION	64%	64%	
16.1 Gestión de incidentes de seguridad de la información y mejoras	64%	64%	
16.1.1 Responsabilidades y procedimientos	60%	60%	
16.1.2 Notificación de los eventos de seguridad de la información	60%	60%	
16.1.3 Notificación de puntos débiles de la seguridad	60%	60%	

16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	65%	65%	
16.1.5 Respuesta a incidentes de seguridad de la información	75%	75%	
16.1.6 Aprendizaje de los incidentes de seguridad de la información	60%	60%	
16.1.7 Recopilación de evidencias	65%	65%	
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	68%	88%	
17.1 Continuidad de la seguridad de la información	60%	100%	Proceso de continuidad del negocio
17.1.1 Planificación de la continuidad de la seguridad de la información	60%	100%	Proceso de continuidad del negocio
17.1.2 Implementar la continuidad de la seguridad de la información	60%	100%	Copias de Respaldo/Proceso de continuidad del negocio
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	60%	100%	
17.2 Redundancias	75%	75%	
17.2.1 Disponibilidad de los recursos de tratamientos de la información	75%	75%	
18. CUMPLIMIENTO	73%	90%	
18.1 Cumplimiento de los requisitos legales y contractuales	73%	79%	
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	80%	80%	
18.1.2 Derechos de propiedad intelectual	80%	90%	Mejora gestión de RH
18.1.3 Protección de los registros de la organización	80%	80%	
18.1.4 Protección y privacidad de la información de carácter personal	70%	90%	Mejora gestión RH
18.1.5 Regulación de los controles criptográficos	55%	55%	
18.2 Revisiones de la seguridad de la información	73%	100%	Revisión del SGSI
18.2.1 Revisiones independientes de la seguridad de la información	75%	100%	
18.2.2 Cumplimiento de las políticas y de las normas de seguridad	70%	100%	
18.2.3 Comprobación del cumplimiento técnico	75%	100%	

ANEXO XV

Tabla de análisis de amenazas/activos después de la implementación de los proyectos.

Grupo de Amenaza	Amenaza	Activo	Frecuencia/Amenaza		Impacto Amenaza				
			ID	Valor	A	C	I	D	T
[N] Desastres naturales									
	[N.1] Fuego								
		[HW] Hardware	MB	**0,002**				100%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				100%	
		[COM]: Redes	MB	**0,002**				100%	
		[I] Instalaciones	MB	**0,002**				100%	
		[P] Personal	MB	**0,002**				100%	
	[N.2] Daños por agua								
		[HW] Hardware	MB	**0,002**				75%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				75%	
		[COM]: Redes	MB	**0,002**				75%	
		[I] Instalaciones	MB	**0,002**				75%	
	[N.*] Desastres naturales								
		[SW] Software	MB	**0,002**				100%	
		[HW] Hardware	MB	**0,002**				100%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				100%	
		[I] Instalaciones	MB	**0,002**				100%	
[I] De origen industrial									
	[I.1] Fuego								
		[SW] Software	MB	**0,002**				100	
		[HW] Hardware	MB	**0,002**				100	

		[AUX] Equipo. Auxiliar	MB	**0,002**				100	
		[I] Instalaciones	MB	**0,002**				100	
	[I.2] Daños por agua								
		[SW] Software	MB	**0,002**				75%	
		[HW] Hardware	MB	**0,002**				75%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				75%	
		[I] Instalaciones	MB	**0,002**				75%	
	[I.*] Desastres industriales								
		[HW] Hardware	MB	**0,002**				75%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				20%	
		[I] Instalaciones	MB	**0,002**				75%	
	[I.3] Contaminación mecánica								
		[HW] Hardware	MB	**0,002**				50%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				50%	
		[I] Instalaciones	MB	**0,002**				50%	
	[I.4] Contaminación electromagnética								
		[HW] Hardware	MB	**0,002**				50%	
		[AUX] Equipo. Auxiliar	MB	**0,002**				50%	
		[I] Instalaciones	MB	**0,002**				50%	
	[I.5] Avería de Origen Físico y lógico								
		[S] Servicios	B	**0,005**				50%	
		[SW] Software	B	**0,005**				50%	
		[HW] Hardware	B	**0,005**				50%	
		[AUX] Equip. Auxiliar	B	**0,005**				20%	
		[COM]: Redes	B	**0,005**				20%	
	[I.6] Corte de suministro eléctrico								
		[HW] Hardware	B	**0,005**				75%	

		[AUX] Equip. Auxiliar	B	**0,005**				50%	
	[I.7] Condiciones inadecuadas de temperatura o humedad								
		[HW] Hardware	B	**0,005**				50%	
		[AUX] Eqp. Auxiliar	B	**0,005**				20%	
		[COM]: Redes	B	**0,005**				20%	
	[I.8] Fallo de servicios de comunicaciones								
		[S] Servicios	M	**0,016**				100%	
		[SW] Software	M	**0,016**				100%	
		[HW] Hardware	M	**0,016**				100%	
		[AUX] Eqp. Auxiliar	M	**0,016**				100%	
		[COM]: Redes	M	**0,016**				20%	
		[AUX] Equipo. Auxiliar	B	**0,005**				20%	
		[HW] Hardware	MB	**0,002**				75%	
	[I.11] Emanaciones electromagnéticas								
		[HW] Hardware	MB	**0,002**		50%			
		[AUX] Equipo Auxiliar	MB	**0,002**		20%			
		[COM]: Redes	MB	**0,002**		20%			
		[I] Instalaciones	MB	**0,002**		20%			
[E] Errores y fallos no intencionados									
	[E.1] Errores de los usuarios								
		[D] Datos- Info	M	**0,016**		5%	5%	5%	
		[S] Servicios	M	**0,016**		5%	5%	5%	
		[SW] Software	M	**0,016**		5%	5%	5%	
	[E.2] Errores del administrador								
		[D] Datos- Info	M	**0,016**		20%	20%	20%	
		[S] Servicios	M	**0,016**		20%	20%	20%	

		[SW] Software	M	**0,016**		20%	20%	20%	
		[HW] Hardware	M	**0,016**		20%	20%	20%	
		[COM]: Redes	M	**0,016**		20%	20%	20%	
	[E.3] Errores de monitorización								
		[D] Datos- Info	M	**0,016**			50%		75%
	[E.4] Errores de configuración								
		[D] Datos- Info	M	**0,016**			50%		
	[E.7] Deficiencias en la organización								
		[P] Personal	M	**0,016**				75%	
	[E.8] Difusión de SW dañino								
		[SW] Software	MB	**0,002**		75%	50%	75%	
		[D] Datos- Info	MB	**0,002**		50%	50%	50%	
	[E.9] Errores de [re]-encaminamiento								
		[S] Servicios	MB	**0,002**		20%			
		[SW] Software	MB	**0,002**		50			
		[COM]: Redes	MB	**0,002**		50%			
	[E.10] Errores de secuencia								
		[S] Servicios	MB	**0,002**			20%		
		[SW] Software	MB	**0,002**			20%		
		[COM]: Redes	MB	**0,002**			20%		
	[E.15] Alteración accidental de la información								
		[D] Datos- Info	MB	**0,002**			50%		
		[S] Servicios	MB	**0,002**			5%		
		[SW] Software	MB	**0,002**			5%		
		[COM]: Redes	MB	**0,002**			5%		
		[I] Instalaciones	MB	**0,002**			5%		
	[E.18] Destrucción de la información								

		[D] Datos- Info	MB	**0,002**			100%		
		[S] Servicios	MB	**0,002**			75%		
		[SW] Software	MB	**0,002**			75%		
		[AUX] Equipo Auxiliar	MB	**0,002**			75%		
		[COM]: Redes	MB	**0,002**			20%		
		[I] Instalaciones	MB	**0,002**			5%		
	[E.19] Fugas de información								
		[D] Datos- Info	M	**0,016**		100%			
		[S] Servicios	M	**0,016**		50%			
		[SW] Software	M	**0,016**		50%			
		[COM]: Redes	M	**0,016**		50%			
		[I] Instalaciones	M	**0,016**		20%			
		[P] Personal	M	**0,016**		75%			
	[E.20] Vulnerabilidades de los programas (SW)								
		[SW] Software	MB	**0,002**		50%	50%	75%	
		[SW] Software	B	**0,005**			20%	75%	
		[HW] Hardware	B	**0,005**				75%	
		[AUX] Equipo Auxiliar	B	**0,005**				75%	
	[E.24] Caída del sistema por agotamiento de recursos								
		[S] Servicios	B	**0,005**				100%	
		[HW] Hardware	B	**0,005**				100%	
		[COM]: Redes	B	**0,005**				100%	
	[E.25] Perdida de equipos								
		[HW] Hardware	B	**0,005**		100%		100%	
	[E.28] Indisponibilidad del personal								
		[P] Personal	B	**0,005**				75%	

[A] Ataques intencionados									
	[A.3]Manipulación de los registros de actividad (log)								
		[D] Datos- Info	MB	**0,002**			75%		75%
	[A.4]Manipulación de la configuración								
		[D] Datos- Info	MB	**0,002**		50%	75%		75%
	[A.5]Suplantación de la identidad del usuario								
		[D] Datos- Info	B	**0,005**	100%	75%		50%	
		[S] Servicios	B	**0,005**	75%	75%		50%	
		[SW] Software	B	**0,005**	75%	75%		50%	
		[COM]: Redes	B	**0,005**	75%	75%		50%	
	[A.6]Abuso de privilegios de acceso								
		[D] Datos- Info	B	**0,005**		100%	50%	50%	
		[S] Servicios	B	**0,005**		75%			
		[SW] Software	B	**0,005**		75%	50%	50%	
		[HW] Hardware	B	**0,005**		75%	50%	50%	
		[COM]: Redes	B	**0,005**		75%	50%	50%	
	[A.7]Uso no previsto								
		[D] Datos- Info	MB	**0,002**		20%	20%	20%	
		[S] Servicios	MB	**0,002**		20%	20%	20%	
		[SW] Software	MB	**0,002**		20%	20%	20%	
		[HW] Hardware	MB	**0,002**		20%	20%	20%	
		[AUX] Equipo Auxiliar	MB	**0,002**		20%	20%	20%	
		[COM]: Redes	MB	**0,002**		20%	20%	20%	
		[I] Instalaciones	MB	**0,002**		20%	20%	20%	
	[A.8]Difusión de software dañino								
		[SW] Software	MB	**0,002**		75%	75%	75%	
	[A.9] [Re-]encaminamiento de mensajes								
		[S] Servicios	MB	**0,002**		50%			
		[SW] Software	MB	**0,002**		50%			

		[COM]: Redes	MB	**0,002**		50%			
	[A.10]Alteración de secuencia								
		[S] Servicios	MB	**0,002**			20%		
		[SW] Software	MB	**0,002**			20%		
		[COM]: Redes	MB	**0,002**			20%		
	[A.11]Acceso no autorizado								
		[D] Datos- Info	M	**0,016**		100%	75%		
		[S] Servicios	M	**0,016**		50%	50%		
		[SW] Software	M	**0,016**		25%	25%		
		[HW] Hardware	M	**0,016**		50%	50%		
		[AUX] Equipo Auxiliar	M	**0,016**		20%	20%		
		[COM]: Redes	M	**0,016**		50%	50%		
		[I] Instalaciones	M	**0,016**		20%	20%		
	[A.12]Análisis de trafico								
		[COM]: Redes	B	**0,005**		100%			
	[A.13]Repudio								
		[D] Datos- Info	MB	**0,002**			50%		100%
		[S] Servicios	MB	**0,002**			50%		100%
	[A.14]Interceptación de información (escucha)								
		[COM]: Redes	MB	**0,002**		100%			
	[A.15]Modificación deliberada de la información								
		[D] Datos- Info	MB	**0,002**			100%		
		[S] Servicios	MB	**0,002**			20%		
		[SW] Software	MB	**0,002**			20%		
		[COM]: Redes	MB	**0,002**			20%		
		[I] Instalaciones	MB	**0,002**			20%		
	[A.18]Destrucción de información								
		[D] Datos- Info	MB	**0,002**				100%	

		[S] Servicios	MB	**0,002**				50%	
		[SW] Software	MB	**0,002**				20%	
		[I] Instalaciones	MB	**0,002**				20%	
	[A.19]Divulgación de información								
		[D] Datos- Info	B	**0,005**		75%			
		[S] Servicios	B	**0,005**		50%			
		[SW] Software	B	**0,005**		50%			
		[COM]: Redes	B	**0,005**		20%			
		[I] Instalaciones	B	**0,005**		20%			
	[A.22]Manipulación de programas								
		[SW] Software	MB	**0,002**		75%	50%	75%	
	[A.23]Manipulación de los equipos								
		[HW] Hardware	B	**0,005**		50%		50%	
		[AUX] Equipo Auxiliar	B	**0,005**		50%		50%	
	[A.24]Denegación de servicio								
		[S] Servicios	MB	**0,002**				100%	
		[HW] Hardware	MB	**0,002**				100%	
		[COM]: Redes	MB	**0,002**				100%	
	[A.25]Robo								
		[HW] Hardware				20%		100%	
		[AUX] Equipo Auxiliar				20%		100%	
	[A.26]Ataque destructivo								
		[HW] Hardware	B	**0,005**				100%	
		[AUX] Equipo Auxiliar	B	**0,005**				100%	
		[I] Instalaciones	B	**0,005**				100%	
	[A.27]Ocupación enemiga								
		[I] Instalaciones	MB	**0,002**		20%		100%	
	[A.28]Indisponibilidad del								

	personal								
		[P] Personal	A	**0,071**				100%	
	[A.29]Extorsión								
		[P] Personal	MB	**0,002**		20%	20%	20%	
	[A.30]Ingeniería social (picaresca)								
		[P] Personal	MB	**0,002**		20%	20%	20%	

ANEXO XVI

Tabla de valoración de los riesgos después de la implementación de los proyectos

Tipo	Activo	Freq	Valor	IMPACTO POTENCIAL					RIESGO				
				A	C	I	D	T	A	C	I	D	T
[SW.1]	Aplicación de gestión de datos clientes	M	0,016	4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[SW.2]	Aplicación de gestión de acceso de usuarios a las distintas aplicaciones			4	6	4	9	0	0,06	0,10	0,06	0,14	0
[SW.3]	Aplicación de gestión de los datos personales de los empleados de la empresa			4	6	4	9	0	0,06	0,10	0,06	0,14	0
[SW.4]	Aplicación de gestión de contratos de los clientes individuales			4	6	4	8	0	0,06	0,10	0,06	0,13	0
[SW.5]	Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas			4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[SW.6]	Aplicación de gestión de contratos empresariales – seguros de grupo			4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[SW.7]	Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos			4	6	4	9	0	0,06	0,10	0,06	0,14	0
[SW.8]	Aplicación contable de la empresa			4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[SW.9]	Servidor de documentos de desarrollo			2,5	3,75	2,5	7	0	0,04	0,06	0,04	0,11	0
[SW.10]	Servidor de documentos en TST			3,5	5,25	3,5	7	0	0,06	0,08	0,06	0,11	0
[SW.11]	Servidor de documentos en INT			4	6	4	8	0	0,06	0,10	0,06	0,13	0
[SW.12]	Servidor de documentos en PRD			4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[SW.13]	Servidor de aplicaciones de desarrollo			2,5	3,75	2,5	5	0	0,04	0,06	0,04	0,08	0
[SW.14]	Servidor de aplicaciones de test			3	4,5	3	6	0	0,05	0,07	0,05	0,10	0
[SW.15]	Servidor de aplicaciones de integración			3,5	5,25	3,5	7	0	0,06	0,08	0,06	0,11	0
[SW.16]	Servidor de aplicaciones de producción			4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[SW.17]	SGBD Oracle en desarrollo			2,5	3,75	2,5	5	0	0,04	0,06	0,04	0,08	0
[SW.18]	SGBD Oracle en test			2,5	3,75	2,5	7	0	0,04	0,06	0,04	0,11	0

[SW.19]	SGBD Oracle en integración			3,5	6	4	7	0	0,06	0,10	0,06	0,11	0
[SW.20]	SGBD Oracle en producción			4,5	6,75	4,5	9	0	0,07	0,11	0,07	0,14	0
[HW.1]	Servidor de aplicaciones internas/finanzas/admini/compta	M	0,016	0	8	1,6	9	0	0	0,13	0,03	0,14	0
[HW.2]	Servidores DNS			0	7	1,6	9	0	0	0,11	0,03	0,14	0
[HW.3]	Servidores DB Oracle prod			0	9	1,8	9	0	0	0,14	0,03	0,14	0
[HW.4]	Servidores DB Oracle dev			0	4	1	5	0	0	0,06	0,02	0,08	0
[HW.5]	Servidores DB Oracle test			0	5	1	7	0	0	0,08	0,02	0,11	0
[HW.6]	Servidores DB Oracle int			0	8	1,6	9	0	0	0,13	0,03	0,14	0
[HW.7]	Servidores de e-comerce			0	0	0	7	0	0	0	0	0,11	0
[HW.8]	Routers			0	0	0	8	0	0	0	0	0,13	0
[HW.9]	Servidores de correo			0	0	0	8	0	0	0	0	0,13	0
[HW.10]	Servidores de Desarrollo			0	0	0	5	0	0	0	0	0,08	0
[HW.11]	Servidores de Test			0	0	0	7	0	0	0	0	0,11	0
[HW.12]	Servidores de Integración			0	0	0	9	0	0	0	0	0,14	0
[HW.13]	Servidores de Producción			0	0	0	9	0	0	0	0	0,14	0
[HW.14]	PC Portables			0	0	0	8	0	0	0	0	0,13	0
[HW.15]	PC de escritorio fijas			0	0	0	5	0	0	0	0	0,08	0
[HW.16]	Tabletas			0	0	0	5	0	0	0	0	0,08	0
[HW.17]	Teléfonos fijos			0	0	0	3	0	0	0	0	0,05	0
[HW.18]	Teléfonos móviles			0	0	0	4	0	0	0	0	0,06	0
[HW.19]	Dispositivos de conexión VPN			0	0	0	8	0	0	0	0	0,13	0
[HW.20]	Rack de comunicaciones			0	0	0	8	0	0	0	0	0,13	0
[HW.21]	Switchs			0	0	0	8	0	0	0	0	0,13	0
[HW.22]	Firewalls			0	0	0	7	0	0	0	0	0,11	0
[HW.23]	Sistema Wifi			0	0	0	8	0	0	0	0	0,13	0
[HW.24]	Cableado de la red			0	0	0	8	0	0	0	0	0,13	0
[HW.25]	Cámaras de vigilancia			0	0	0	5	0	0	0	0	0,08	0
[HW.26]	Servidor de documentos			0	8	1,6	8	0	0	0,13	0,03	0,13	0

[HW.27]	Servidor de copias de seguridad			0	7	1,6	9	0	0	0,11	0,03	0,14	0
[HW.28]	Multiservidores de impresión/scanner/fotocopias			0	0	0	5	0	0	0	0	0,08	0
[I.1]	Centro de procesamiento de datos	M	0,002	0	0	0	9	0	0	0	0	0,02	0
[I.2]	Salas de Reuniones			0	0	0	5	0	0	0	0	0,01	0
[I.3]	Puestos de trabajo del personal – open spaces			0	0	0	8	0	0	0	0	0,02	0
[I.4]	Puestos de trabajo bajo seguro			0	0	0	7	0	0	0	0	0,01	0
[I.5]	Oficinas de los directivos			0	0	0	6	0	0	0	0	0,01	0
[I.6]	Salas de impresión			0	0	0	4	0	0	0	0	0,01	0
[I.7]	Unidades de apoyo a los servicios			0	0	0	4	0	0	0	0	0,01	0
[I.8]	Espacios de almacenamiento de los racks			0	0	0	8	0	0	0	0	0,02	0
[I.9]	Espacio de almacenamiento de documentos papel seguros			0	0	0	8	0	0	0	0	0,02	0
[D.1]	Código fuentes aplicaciones de gestión de contratos	M	0,005	6,75	7,5	7,5	7,5	6,75	0,03	0,04	0,04	0,04	0,03
[D.2]	Código fuente aplicaciones de gestión de usuarios			6,75	7,5	7,5	7,5	6,75	0,03	0,04	0,04	0,04	0,03
[D.3]	Código fuente aplicaciones de gestión de datos de empleados			6,75	7,5	7,5	7,5	6,75	0,03	0,04	0,04	0,04	0,03
[D.4]	Código fuente aplicación de gestión de acceso de usuarios / aplicaciones			6,75	7,5	7,5	7,5	6,75	0,03	0,04	0,04	0,04	0,03
[D.5]	Datos de clientes individuales			6,75	7,5	6,75	6,75	6	0,03	0,04	0,03	0,03	0,03
[D.6]	Datos de clientes empresariales			6,75	7,5	6,75	6,75	6	0,03	0,04	0,03	0,03	0,03
[D.7]	Datos de clientes independientes			6,75	7,5	6,75	6,75	6	0,03	0,04	0,03	0,03	0,03
[D.8]	Datos de los empleados de la empresa			6	7,5	6,75	5,25	6	0,03	0,04	0,03	0,03	0,03
[D.9]	Datos de acceso a las aplicaciones (roles y responsabilidades)			6	6,75	6	6,75	6,75	0,03	0,03	0,03	0,03	0,03
[D.10]	Documentos de clientes			6	6	6	6,75	6	0,03	0,03	0,03	0,03	0,03
[D.11]	Documentos de empleados			6	6	6	6,75	6	0,03	0,03	0,03	0,03	0,03
[D.12]	Documentos otros			3,75	4,5	5,25	5,25	6	0,02	0,02	0,03	0,03	0,03
[D.13]	Datos de soporte y licencias			3,75	4,5	5,25	5,25	6	0,02	0,02	0,03	0,03	0,03
[D.14]	Log de servidores y log de clientes			6,75	7,5	7,5	7,5	6,75	0,03	0,04	0,04	0,04	0,03
[D.15]	Backup de DB users			6	6	6,75	6,75	6,75	0,03	0,03	0,03	0,03	0,03
[D.16]	Documentos en papel (contratos)			6	6	6,75	6,75	6,75	0,03	0,03	0,03	0,03	0,03

[D.17]	Backup código fuente			6	6	6,75	6,75	6,75	0,03	0,03	0,03	0,03	0,03
[D.18]	Backuo de DB Clientes			6	6	6,75	6,75	6,75	0,03	0,03	0,03	0,03	0,03
[D.19]	Backup DB empleados			6	6	6,75	6,75	6,75	0,03	0,03	0,03	0,03	0,03
[D.20]	Datos de configuración			6	6	6,75	6,75	6,75	0,03	0,03	0,03	0,03	0,03
[COM.1]	Internet	M	0,016	0	8	1,6	8	0	0	0,13	0,03	0,13	0
[COM.2]	Red inalámbrica			0	8	1,6	7	0	0	0,13	0,03	0,11	0
[COM.3]	RED telefónica			0	5	1	7	0	0	0,08	0,02	0,11	0
[COM.4]	Cableado telecomunicaciones			0	0	0	8	0	0	0	0,00	0,13	0
[COM.5]	Telefonía móvil			0	0	0	7	0	0	0	0,00	0,11	0
[COM.6]	Red Local				8	1,6	9	0	0	0,13	0,03	0,14	0
[COM.7]	Cableado eléctrico			0	0	0	0	0	0	0	0,00	0,00	0
[S.1]	Servicio Web	M	0,016	3,5	3,5	3,5	4	6	0,06	0,06	0,06	0,06	0,10
[S.2]	Servicio de aplicaciones			0	0	0	4,5	0	0	0	0	0,07	0
[S.3]	Servicios de archivos			4	3	4	3,5	6	0,06	0,05	0,06	0,06	0,10
[S.4]	Servicios de documentos			4	3	4	3,5	6	0,06	0,05	0,06	0,06	0,10
[S.5]	Servicios DNS			3,5	4	4	4	5,25	0,06	0,06	0,06	0,06	0,08
[S.6]	Servicios email			3,5	3,5	4	3	4,5	0,06	0,06	0,06	0,05	0,07
[S.7]	Servicio comunicaciones			4	4	4	4,5	6	0,06	0,06	0,06	0,07	0,10
[S.8]	Portal interno			3,5	3,5	3,5	3,5	5,25	0,06	0,06	0,06	0,06	0,08
[S.9]	Portal Externo			4,5	4	4	4,5	6,75	0,07	0,06	0,06	0,07	0,11
[AUX.1]	Lockers	M	0,016	0	0	0	6	0	0	0	0	0,10	0
[AUX.2]	Multiprinters			0	0	0	5	0	0	0	0	0,08	0
[AUX.3]	Recursos varios (material de escritorio, maletas, …)			0	0	0	3	0	0	0	0	0,05	0
[AUX.4]	Televisores			0	0	0	3	0	0	0	0	0,05	0
[AUX.5]	Equipos de sonido y proyección			0	0	0	3	0	0	0	0	0,05	0
[AUX.6]	Pantallas			0	0	0	3	0	0	0	0	0,05	0
[AUX.7]	Cableado eléctrico			0	0	0	8	0	0	0	0	0,13	0
[AUX.8]	Mobiliario			0	0	0	7	0	0	0	0	0,11	0

[P.1]	Director General	M	0,016	0	0	0	9	0	0	0	0	0,14	0
[P.2]	Director IT			0	0	0	8	0	0	0	0	0,13	0
[P.3]	Director operaciones			0	0	0	9	0	0	0	0	0,14	0
[P.4]	Director de recursos humanos			0	0	0	4	0	0	0	0	0,06	0
[P.4]	Directos Riesgos			0	0	0	4	0	0	0	0	0,06	0
[P.5]	Director Finanzas			0	0	0	7	0	0	0	0	0,11	0
[P.6]	Director Marketing y ventas			0	0	0	4	0	0	0	0	0,06	0
[P.7]	Personal de desarrollo de las aplicaciones			0	0	0	7	0	0	0	0	0,11	0
[P.8]	Gestionaros de contratos/Business Experto			0	0	0	9	0	0	0	0	0,14	0
[P.9]	Personal RH			0	0	0	4	0	0	0	0	0,06	0
[P.10]	Administrador de la aplicación			0	0	0	8	0	0	0	0	0,13	0
[P.11]	Técnicos de soporte buSiness			0	0	0	7	0	0	0	0	0,11	0
[P.12]	Agentes de ventas			0	0	0	5	0	0	0	0	0,08	0
[P.13]	Personal Comercial			0	0	0	5	0	0	0	0	0,08	0
[P.14]	Personal Fínanzas			0	0	0	8	0	0	0	0	0,13	0
[P.15]	Personal Infraestructura			0	0	0	7	0	0	0	0	0,11	0
[P.16]	Personal Risks			0	0	0	5	0	0	0	0	0,08	0
[P.17]	Administradores de sistemas			0	0	0	7	0	0	0	0	0,11	0
[P.18]	Personal de soporte IT			0	0	0	5	0	0	0	0	0,08	0

ANEXO XVII

NIVEL DE CUMPLIMIENTO ISO/IEC 27002:2013

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
5 POLÍTICAS DE SEGURIDAD			L4	
5.1 Directrices de la Dirección en seguridad de la información	Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.		L4	
5.1.1 Conjunto de políticas para la seguridad de la información	La dirección debe definir y aprobar el documento que define. Publicarlo y comunicarlo a las partes internas y externas.	SI	L4	Existe un documento que define las políticas de seguridad del manejo de la información de la empresa. Este documento ha sido aprobado, publicado y comunicado por el comité de dirección y cuenta con el apoyo de la direcciones. Existe un plan de formación del personal de la empresa. El documento de las políticas es accesible a través de la intranet. Algunos miembros del personal no conocen estas políticas.
5.1.2 Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de la información deberían revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	SI	L4	Existe un plan anual de revisión de las políticas. Así como una directiva que indica que la revisión de efectúa cuando se han introducido cambios que requieren una revisión de la eficacia de las políticas definidas. Sin embargo no se tiene registro de una revisión de las políticas reciente.
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			L3	
6.1 Organización interna	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		L3	
6.1.1 Asignación de responsabilidades para la seguridad de la información	Deberían definirse y asignarse todas las responsabilidades relativas a la seguridad de la información.	SI	L3	Los roles y las responsabilidades están claramente asignadas. El security officer depende directamente de la dirección. Los responsables de los activos están claramente identificados. Existe un documento en el que figuran los diferentes roles y responsabilidades. Sin embargo, no existe registro de los detalles de las responsabilidades. No existen niveles de autorización definidos.

6.1.2 Segregación de tareas	Las funciones y áreas de responsabilidad deberían segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	**SI**	L3	Los activos de la organización tienen un solo propietario. Ninguna persona está facultada para solicitar, autorizar, utilizar y/o modificar un activo. Existen procedimientos definidos para ello. Se deben pasar por cuatro etapas clave como aprobación, ejecución, registro y custodia de los diferentes activos y a través de departamentos o unidades independientes. Sin embargo, existen registros de excepciones que no han respetado por estos procedimientos.
6.1.3 Contacto con las autoridades	Deberían mantenerse los contactos apropiados con las autoridades pertinentes.	**SI**	L3	La empresa tiene un plan de comunicación con autoridades como la Comisión para la protección de la privacidad, la autoridad sectorial, la policía y el CERT. Este plan especifica qué comunicar, a quiénes y cuando comunicar. Dentro del directorio de autoridades con las cuales comunicar se tiene indicado los direcciones de contacto. Sin embargo no se registran todas las comunicaciones con las autoridades. El personal no documenta todas estas comunicaciones. No existe un template para el registro de las comunicaciones. Este plan no ha sido revisado recientemente.
6.1.4 Contacto con grupos de interés especial	Deberían mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	**SI**	L3	La empresa tiene suscripciones a dos revistas especializadas: SC magazine, CSO y IEEE computer Security and privacy. El security officer tiene planificado cada año una formación/conferencia dentro del área de la seguridad. El security officer debe escribir cada anio por lo menos un articulo sobre la seguridad para publicarlo en la revista digital de la empresa que se publica a través del portal interno. Sin embargo, no existe
6.1.5 Seguridad de la información en la gestión de proyectos	La seguridad de la información debería tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	**NO**	L2	No existe una directiva clara que especifique que la seguridad debe ser tratada dentro la gestión de proyectos. Hoy en día el tratamiento de la seguridad de la información dentro de los proyectos depende de la iniciativa de los responsables de proyectos.
6.2 Dispositivos para movilidad y teletrabajo	Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles			
6.2.1 Política de uso de dispositivos para movilidad	Se debería adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	**NO**	L2	Existe un documento de uso de dispositivos móviles. Cada empleado que hace uso de un dispositivo móvil debe conocer y aplicar la reglamentación para estos dispositivos. Así mismo cada empleado se hace responsable del dispositivo y de la información que este dispone. - Existen registros de un numero importante de incidentes de Seguridad durante el teletrabajo.
6.2.2 Teletrabajo	Se debería implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	**NO**	L3	Existe un documento que reglamenta el teletrabajo. Todos los empleados de la empresa pueden trabajar dos días a la semana y estos se hacen responsables de la seguridad de los equipos de teletrabajo y la información a la que acceden a través de sus accesos asignados. Se han implementado medidas de seguridad que permitan el teletrabajo y que minimicen los accesos no autorizados. Sin emabargo existen registros de un numero importante de incidentes de Seguridad durante el teletrabajo.
7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS			L3	

7.1 Antes de la contratación	Para asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.		L3	
7.1.1 Investigación de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debería llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debería ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	**SI**	L3	Dentro de los procedimientos que sigue la empresa antes de la contratación de personal (interno, externo o terceros con los que tiene una relación profesional) solicita la certificación de antecedentes de acuerdo a las regulaciones existentes. Dependiendo de la información a la cual va a tener acceso y los riesgos que conlleva la misma, la empresa hace la verificación de los antecedentes. Existen registros que en algunos casos estas verificaciones se realizan despues de que el personal ha sido ya contratado.
7.1.2 Términos y condiciones de contratación	Como parte de sus obligaciones contractuales, los empleados y contratistas deberían establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	**SI**	L3	Todo contrato de trabajo que se firma incluye la clausula de aceptación de los términos y las condiciones concernientes a la seguridad de la información y la aplicación de las políticas de la seguridad de la información. Así mismo esta presente la clausula de confidencialidad y no revelación de la información. Todo personal recibe el reglamento de trabajo junto con su trato. Todo personal debe seguir una formación virtual sobre la seguridad de la información y aprobar el test de evaluación. Esta formación la debe realizar dentro la primera semana de trabajo. Sin embargo no existe registro sobre la verificación de si la persona ha hecho esta formación dentro de los tiempos establecidos.
7.2 Durante la contratación	Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.			
7.2.1 Responsabilidades de gestión	La dirección debería exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	**SI**	L3	La empresa ha dado las directivas sobre la importancia de la seguridad de la información y las consecuencias del no respecto de las políticas definidas. Los empleados y contratistas tienen definido un programa de formación / información / concientización sobre políticas y procedimientos y sus responsabilidades pero existen registros que muestran que no están completamente consientes sobre la importancia de gestión la información de manera segura.
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	**SI**	L3	La empresa tiene un plan de formación/actualización anual para cada empleado en temas relacionados a la seguridad de la información. Esta formación es obligatoria y se la realiza una vez al año como mínimo. Sin embargo no esta claro qué procedimiento seguir cuando se identifica violaciones o no respeto de los políticas definidas. No se tiene claro tampoco a quien hacer los reportes en caso de violaciones o no respeto.
7.2.3 Proceso disciplinario	Debería existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	**SI**	L3	Existe un proceso disciplinario definido y que es de conocimiento de los empleados. La formación que tienen planificada aborda el tema del proceso disciplinario. Este documento está para el personal y puede ser accedido a través del portal interno de la empresa. Existe una persona responsables de RRHH que aplica el proceso disciplinario. Sin embargo existe evidencia que existe personal que desconoce la existencia de los procesos disciplinarios.

7.3 Cese o cambio de puesto de trabajo	Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.			
7.3.1 Cese o cambio de puesto de trabajo	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deberían definir, comunicar al empleado o contratista y se deberían cumplir.	**SI**	L3	En el contrato de trabajo se establecen las responsabilidades en materia de seguridad vigentes después del cambio o finalización del empleo. El personal conoce estas responsabilidades y las ha asumido. Sin embargo existe evidencia de infracciones.
8. GESTIÓN DE ACTIVOS			L3	
8.1 Responsabilidad sobre los activos	Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		L3	
8.1.1 Inventario de activos	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.	**SI**	L3	Se realizó la identificación de los activos para los procesos incluidos dentro del alcance del SGSI. Sin embargo los inventarios de activos no están completos debido a que no son actualizados con frecuencia.
8.1.2 Propiedad de los activos	Todos los activos que figuran en el inventario deberían tener un propietario.	**SI**	L3	Los activos que se han identificado tiene los propietarios asociados. Estos son los responsables de su clasificación y de definir las restricciones de acceso. Estos propietarios definen el manejo seguro y el borrado seguro Sin emabrgo no existe evidencia de actualizaciones recientes.
8.1.3 Uso aceptable de los activos	Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	**SI**	L3	Existe un documento general que da los lineamientos sobre el uso aceptable de grupos de activos. Existe un documento general que describe el uso aceptable de la información dentro de la empresa. Sin embargo no existe evidencia de revisiones frecuentes.
8.1.4 Devolución de activos	Todos los empleados y terceras partes deberían devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	**SI**	L3	Existe un procedimiento definido de devolución de activos cuando la relación laboral termina. Comprende un checklist de todos los activos que se le han asignado y que deben ser devueltos. Se suprimen los accesos y se recuperan los medios de almacenamiento. Se inspeccionan las alertas ante movimientos masivos de información. Sin embargo existe evidencia de activos no devueltos.
8.2 Clasificación de la información	Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.		L3	
8.2.1 Directrices de clasificación	La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	**SI**	L3	Los responsables de la información han definido directrices para clasificar la información. Estas directrices han sido aprobadas y son comunicadas. Sin embargo no hay registros de revisiones recientes sobre las directrices.
8.2.2 Etiquetado y manipulado de la información	Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	**SI**	L3	Los responsables de la información, han definido unos criterios para clasificar la información. Después del análisis de riesgos se propone el proyecto de la clasificación de la información. Se han definido procedimientos para etiquetar la información.

8.2.3 Manipulación de activos	Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	**SI**	L3	Se han definido y comunicado los procedimientos de manipulación de la información. Sin embargo existe evidencia de que estos procedimientos no son conocidos por todos y por ende no aplicados por todos.
8.3 Manejo de los soportes de almacenamiento	Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada.		L3	
8.3.1 Gestión de soportes extraíbles	Se deberían implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	**SI**	L3	Existen procedimientos definidos para la gestión de los soportes extraíbles. Estos procedimientos están aprobados y han sido comunicados. Sin embargo no existe registro de la aplicación de estos procedimientos por parte del personal.
8.3.2 Eliminación de soportes	Los soportes deberían eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	**SI**	L3	Existe un documento que detalla un procedimiento formal para el borrado de forma segura algunos soportes de almacenamiento. Sin embargo no se ha encontrado un registro de los soportes borrados que date del año pasado.
8.3.3 Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	**SI**	L3	Existen procedimientos definidos para el transporte de forma segura de la información. Existe evidencia del no respeto de estos procedimientos y usos indebidos.
9. CONTROL DE ACCESOS			L3	
9.1 Requisitos de negocio para el control de accesos	Limitar el acceso a los recursos de tratamiento de información y a la información.		L4	
9.1.1 Política de control de accesos	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	**SI**	L4	Existen reglas de acceso definidas para los activos de acuerdo a los roles y responsabilidades de los usuarios. Los controles implementados son lógicos y físicos. No se otorgan accesos sin previa autorización por los responsables de los activos y de acuerdo a los roles y responsabilidades definidos. Existen revisiones planificadas.
9.1.2 Control de acceso a las redes y servicios asociados	Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	**SI**	L3	Existe un documento sobre las políticas de uso de las redes y los servicios de red. Estas políticas están en coherencia con las reglas de acceso definidas.
9.2 Gestión de acceso de usuario	Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.			
9.2.1 Registro de acceso y baja de usuarios	Debería implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso .	**SI**	L3	Existe procedimientos formales para la asignación de identificadores únicos a los usuarios, así como para la eliminación e inhabilitación de los identificadores cuando no son necesarios.
9.2.2 Provisión de acceso de usuario	Debería implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	**SI**	L3	Existen procedimientos formales definidos para la asignación y revocación de derechos de acceso para los usuarios.

9.2.3 Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debería estar restringida y controlada.	**SI**	L3	La asignación y el uso de privilegios de acceso es restringido y controlado. El acceso de los usuarios depende de los roles y responsabilidades, así como de un proceso formal de autorización por los responsables. Dependiendo del trabajo que realizan, dos personas con el mismo, perfil, rol y responsabilidad pueden tener accesos diferentes. Todas estas autorizaciones de accesos son registradas. Existen revisiones periódicas de los accesos privilegiados.
9.2.4 Gestión de la información secreta de autenticación de los usuarios	La asignación de la información secreta de autenticación debería ser controlada a través de un proceso formal de gestión.	**NO**	L3	La gestión de la información secreta de la autenticación se controla a través de un proceso formal. Sin embargo este proceso formal no requiere la firma de un compromiso por parte del usuario. La información de autenticación secreta temporal del usuario no sigue ningún procedimiento definido.
9.2.5 Revisión de los derechos de acceso del usuario	Los propietarios de los activos deberían revisar los derechos de acceso de usuario a intervalos regulares.	**SI**	L3	Existe un plan anual de revisión de los derechos de acceso de los diferentes usuarios. Así mismo existe un procedimiento formal de revisión de accesos de un usuario ante cambios dentro de sus funciones, promociones, movimientos, retiros.
9.2.6 Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deberían ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	**SI**	L3	Existen procedimientos formales para retirar o reasignar accesos a la información y a los recursos cuando existen cambios en el empleo. Esto equivale a retirar accesos y asignar nuevos accesos de acuerdo a su nuevo posición de trabajo. Los accesos privilegiados y/o compartidos son reinicializados y comunicados a los destinatarios.
9.3 Responsabilidades del usuario	Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.		L4	
9.3.1 Uso de la información secreta de la autenticación	Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	**SI**	L4	Existen directivas dentro de la organización sobre las practicas en materia de manejo de claves. Este tema forma parte del temario de la formación en seguridad que los empleados siguen. Estas directivas se encuentran definidas dentro de las políticas de seguridad de la empresa.
9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones.		L3	
9.4.1 Restricción de acceso a la información	Se debería restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	**SI**	L3	Existe una política de gestión de acceso para las aplicaciones y la información. Para asignar accesos tanto a las aplicaciones como a la información se disponen de matrices de acceso definidas, sin embargo existe evidencias de usuarios que tienen accesos no autorizados.
9.4.2 Procedimientos seguros de inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debería controlar por medio de un procedimiento seguro de inicio de sesión.	**NO**	L3	El procedimiento seguro de inicio de sesión no esta implantado en todos las aplicaciones que lo requieren.

9.4.3 Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas.	**NO**	L3	Se han definido sistemas de gestión de contraseñas. Existe evidencia de que los sistemas de gestión de contraseñas no están implementados en todos los sistemas ni en todas las aplicaciones. Existen diferentes sistemas de gestión de contraseña implementados
9.4.4 Uso de utilidades con privilegios del sistema	Se debería restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	**SI**	L3	El uso de utilidades con privilegios es controlado y restringido. Los usuarios no pueden hacer instalaciones en sus equipos sin la intervención del equipo a cargo. Toda instalación requiere una autorización. Sin embargo existen reportes sobre usuarios que han logrado instalar ciertos programas no autorizados.
9.4.5 Control de acceso al código fuente de los programas	Se debería restringir el acceso al código fuente de los programas.	**SI**	L3	Existen procedimientos establecidos para asignar los accesos a los códigos fuente y documentación de los programas y/o aplicaciones. Existen diferentes ambientes de desarrollo y de prueba. Sin embargo existe evidencia de accesos a estas fuentes por parte de personal de soporte. Existe evidencia de que no se aplican estos procedimientos.
10. CRIPTOGRAFIA			L3	
10.1 Controles criptográficos	Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		L3	
10.1.1 Política de uso de los controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	**NO**	L3	La política esta definida dentro de las políticas de seguridad de la empresa. No existe registro de uso o de difusión de esta política. No existe registro de una revisión en los últimos 3 años de la política.
10.1.2 Gestión de claves	Se debería desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	**SI**	L3	Existe un documento guía sobre el uso, la protección y la duración de las claves de cifrado. Este documento forma parte del cuerpo documental del SGSI de la empresa. Sin embargo no existe evidencia sobre procesos de recuperación de claves, de destrucción de claves.
11. SEGURIDAD FISICA DEL ENTORNO			L3	
11.1 Áreas seguras	Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.		L3	
11.1.1 Perímetro de seguridad física	Se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	**SI**	L3	La empresa tiene bien definidas las áreas y los sistemas de seguridad asociados que dependen del nivel de seguridad que se requiere. Las áreas donde se encuentras la infraestructura tecnológica y/o la información sensible cuentan con controles de acceso físico y vigilancia 24/24, 7/7. Para la seguridad física cuenta con los servicios de una empresa de seguridad externa. Sin embargo existen tarjetas de accessos privilegiados distribuidos sin limite de tiempo.

11.1.2 Controles físicos de entrada	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	**SI**	L3	El acceso a las diferentes áreas es controlada por medio del batch individual. El acceso a las áreas que requieren autorización es realizado bajo autorización y con el registro de la visita. Las visitas se realizan acompañado y con un objetivo preciso a indicar. Sin embargo, se halla registro de accesos autorizados pero que no han seguido el procedimiento formal de autorización.
11.1.3 Seguridad de oficinas, despachos y recursos	Para las oficinas, despachos y recursos, se debería diseñar y aplicar la seguridad física.	**SI**	L3	Las diferentes áreas están bien definidas, y el publico solo tiene acceso al piso 0 donde se encuentra la recepción. El acceso a las otros pisos es por medio de una tarjeta de acceso. LA tarjeta de acceso es configurado de manera a permitir acceso solo a determinadas áreas y en determinados horarios y fechas. Sin embargo existe evidencia de accesos no autorizados.
11.1.4 Protección contra las amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	**SI**	L3	Existen áreas seguras en la segunda sede de la empresa.
11.1.5 El trabajo en áreas seguras	Se deberían diseñar e implementar procedimientos para trabajar en las áreas seguras.	**SI**	L3	Las áreas seguras solo son accesibles bajo autorización y con justificación.
11.1.6 Áreas de carga y descarga	Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	**SI**	L4	Las áreas de carga y descarga son de acceso publico y se encuentran físicamente aisladas de las áreas de trabajo del personal y de las áreas de tratamiento de la información. Para ingresar y salir de estas áreas se necesita de autorización.
11.2 Seguridad de los equipos	Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.		L3	
11.2.1 Emplazamiento y protección de equipos	Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	**SI**	L5	Los equipos de procesamiento de información se encuentran situados en la segunda sede. La protección y la seguridad de las instalaciones esta a cargo de una empresa externa.
11.2.2 Instalaciones de suministro	Los equipos deberían estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	**SI**	L5	La protección de los equipos contra las fallas de alimentación y otras alteraciones esta a cargo de una empresa externa. Sin embargo existe registro de fallas de alimentación en el suministro.
11.2.3 Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.	**SI**	L5	La seguridad del cableado y las telecomunicaciones esta a caro de una empresa externa. Existe registro de deficiencias en la seguridad del cableado.
11.2.4 Mantenimiento de los equipos	Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	**SI**	L5	El mantenimiento de los equipos esta a cargo de una empresa externa.

11.2.5 Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no deberían sacarse de las instalaciones.	**SI**	L3	Existen procedimientos definidos para el retiro de material propiedad de la empresa. Sacar información o equipos fuera de la empresa requiere autorizaciones.
11.2.6 Seguridad de los equipos fuera de las instalaciones	Deberían aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	**SI**	L3	Se han definido directrices para la seguridad de los equipos de la empresa que se encuentran fuera de las instalaciones. El personal tiene conocimiento de estas directrices y se compromete a aplicarlas. Existe evidencia de personal que ha perdido los equipos y que no tiene conocimiento de la as directrices.
11.2.7 Reutilización o eliminación segura de equipos	Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	**SI**	L5	La reutilización y/o eliminación segura de los equipo esta a cargo de una empresa externa.
11.2.8 Equipo de usuario desatendido	Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada.	**NO**	L2	Existen directivas a seguir para asegurar la protección de los equipos que no están atendidos. Existen procedimientos definidos para proteger la información y los equipos desentendidos. Existe evidencia de malas practicas por parte de los usuarios. Muchos tienen sus aplicaciones activas y abiertas aun cuando éstas no están siendo utilizadas.
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	**NO**	L2	La política de clean & clean desk existe y ha sido comunicada a todos los empleados. Sin embargo, existe evidencia de resistencia a la aplicación de estas políticas por un numero considerable de usuarios.
12. SEGURIDAD DE LAS OPERACIONES			L3	
12.1 Procedimientos y responsabilidades operacionales	Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		L3	
12.1.1 Documentación de procedimientos de las operaciones	Deberían documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	**SI**	L3	Existen procedimientos definidos y documentados para las principales actividades operacionales. Esto procedimientos están documentados y están accesibles a través del portal interno de la empresa. Sin embargo no todos los procedimientos operacionales están documentados.
12.1.2 Gestión de cambios	Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deberían ser controlados.	**NO**	L3	Se cuenta con un procedimiento formal de control de cambios y con un comité de gestión de cambios que se reúne para validar las solicitudes tanto en sistemas de información como en infraestructura. Sin embargo se evidencia de cambios realizados sin haber pasado por el procedimiento formal.
12.1.3 Gestión de capacidades	Se debería supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	**NO**	L2	Existen procedimientos automáticos para monitorear y ajustar el uso de ciertos recursos. Sin embargo no existe un plan documentado de gestión de la capacidad de los recursos.
12.1.4 Separación de los recursos de desarrollo, prueba y operaciones	Deberían separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	**SI**	L3	Existen diferentes ambientes de desarrollo, pruebas y producción. Sin embargo muchas veces estos ambientes no son utilizados correctamente. Se ha constatado que existen intervenciones de corrección en el ambiente de producción.

12.2 Protección contra el software malicioso	Asegurar que los recursos de tratamiento de información y la información están protegidos contra el *malware*.		L3	
12.2.1 Controles contra el código malicioso	Se deberían implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	**SI**	L3	La empresa ha implementado controles y ha definido procedimientos de concientización/formación para los usuarios. Existen registros de procedimientos no implementados.
12.3 Copias de seguridad	Evitar la pérdida de datos.		L3	
12.3.1 Copias de seguridad de la información	Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente de acuerdo a la política de copias de seguridad acordada.	**SI**	L3	Existe una política de respaldo definida. Existe un plan de respaldo en implementación. Existen procedimientos definidos para la realización de la copias y la recuperación de los datos. Existe evidencia de la perdida de copias de respaldo.
12.4 Registros y supervisión	Registrar eventos y generar evidencias.		L3	
12.4.1 Registro de eventos	Se deberían registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	**SI**	L3	Esta implementado el registro de los eventos de los usuarios. Este registro es almacenado. Existe evidencia que se revisa periódicamente los eventos y se presenta un informe al responsable de la seguridad. Sin embargo, no existe registro de planes de revisión.
12.4.2 Protección de la información de registro	Los dispositivos de registro y la información del registro deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados.	**SI**	L3	Los registros de los eventos están protegidos y solo pueden ser accedidos por los administradores.
12.4.3 Registros de administración y operación	Se deberían registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	**NO**	L2	Esta implementado el registro de las actividades de los administradores y operadores del sistema. Estos registros son almacenados. Sin embargo no existe evidencia de una revisión reciente de las actividades de administrador, ni un informe sobre el registro de actividades de los administradores del año pasado.
12.4.4 Sincronización del reloj	Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deberían estar sincronizados con una única fuente precisa y acordada de tiempo.	**SI**	L3	Los relojes de todos los sistemas están sincronizados. El controlador de dominio y los sistemas están integrados con un sistema NTP publico. Existen procedimientos de verificación de variación de los relojes y de corrección. Sin embargo no existe evidencia reciente de implementación del procedimiento de verificación.
12.5 Control del software en explotación	Se deberían implementar procedimientos para controlar la instalación del software en explotación.		L3	
12.5.1 Instalación del software en explotación	Se deberían implementar procedimientos para controlar la instalación del software en explotación.	**SI**	L3	Existen procedimientos definidos a seguir para la instalación de un nuevo software. En general las instalaciones se realizan por la unidad responsable de instalaciones. Solo algunos usuarios tienen privilegios para realizar las instalaciones. Sin embargo no se ha encontrado evidencia sobre controles efectuados.
12.6 Gestión de la vulnerabilidad técnica	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.		L3	

12.6.1 Gestión de la vulnerabilidad técnica	Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	**SI**	L3	Este proceso es realizado por una entidad externa y esta planificado. Existe evidencia de vulnerabilidades técnicas identificadas y la adopción de medidas para afrontar las vulnerabilidades. Sin embargo no todos los sistemas de información son evaluados, ni tampoco se afrontan todos los riesgos.
12.6.2 Restricción en la instalación del software	Se deberían establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	**SI**	L3	Existen procedimientos definidos para la instalación de nuevo software por parte de los usuarios. La instalación debe obedecer las reglas definidas. En general los usuarios no son administradores de sus equipos y no pueden realizar instalaciones. Sin embargo existe registro de usuarios con mayores privilegios y que no ha seguidos los procedimientos definidos.
12.7 Consideraciones sobre la auditoria de sistemas de información	Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		L3	
12.7.1 Controles de auditoria de sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberían ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	**SI**	L3	Existe un plan de auditoría para comprobar la seguridad de la organización que incluye auditar los sistemas de información de la organización. Se han acordado requisitos y actividades de auditoria con miras a minimizar el riesgo de interrupciones de los procesos de negocio. Sin embargo existe evidencia de interrupciones de los procesos de negocio.
13. SEGURIDAD DE LAS COMUNICACIONES			L3	
13.1 Gestión de la seguridad de redes	Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.		L3	
13.1.1 Controles de red	Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	**SI**	L3	La implementación de controles que garanticen la seguridad de la información en las redes es externalizada a una empresa especializada. Existe evidencia de un monitoreo continuo sin embargo los reportes del monitoreo reflejan la totalidad de los controles que se especifican. No existe evidencia de seguimiento de estos reportes.
13.1.2 Seguridad de los servicios de red	Se deberían identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	**SI**	L3	La supervisión de la capacidad del proveedor de servicios es externalizado y se tiene acordado que el proveedor debe ser auditado. Se tienen definidas las disposiciones de seguridad necesarias en la red y el cumplimiento de estas disposiciones se encuentra especificadas en los contratos con los proveedores. Sin embargo no existe evidencia de revisiones que la empresa realiza con referencia al cumplimiento de estas especificaciones .
13.1.3 Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas.	**SI**	L3	Se tiene implementada la segregación de las redes en diferentes dominios. La segregación es en función a grupos de usuarios, servicios y sistemas de información. Sin embargo no se tiene evidencia de una revisión o actualización del proceso de segregación reciente.

13.2 Intercambio de información	Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.		L3	
13.2.1 Políticas y procedimientos en intercambio de información	Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	**SI**	L3	Existen políticas, procedimientos y controles formales definidos para el intercambio. Estos han sido comunicados al personal de la empres y la documentación se encuentra disponible a través del portal interno de la empresa. Sin embargo no existe evidencia de revisiones y/o actualizaciones recientes. Asimismo existe evidencia del no respeto de las políticas y/o procedimientos.
13.2.2 Acuerdos de intercambio de información	Deberían establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros. La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.	**SI**	L3	Se ha definido directivas para el proceso de intercambio seguro de la información entre la empresa y terceros. Existen políticas y procedimientos definidos para ello. Sin embargo se evidencia la ausencia de la mención a estas políticas y procedimientos en algunos acuerdos que se han firmado con terceros.
13.2.3 Mensajería electrónica	La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.	**SI**	L3	Se han implementado mecanismos de protección para la mensajería electrónica. Sin embargo existe evidencia de uso de servicios públicos externos por parte de algunos usuarios.
13.2.4 Acuerdos de confidencialidad o no revelación	Deberían identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.	**SI**	L3	La cláusula de confidencialidad y no revelación de la información se encuentra presente en todos los contratos del personal interno, externo, proveedores y otros que prestadores de servicios. Sin embargo existe evidencia de desconocimiento de estos acuerdos por parte de cierto personal de la empresa.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN			L3	
14.1 Requisitos de seguridad en sistemas de información	Garantizar que la seguridad de la información sea 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.		L3	
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Los requisitos relacionados con la seguridad de la información deberían incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	**NO**	L2	Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes no siempre especifican los requisitos relacionados a la seguridad de la información en las etapas iniciales.
14.1.2 Asegurar los servicios de aplicaciones en redes publicas	La información involucrada en aplicaciones que pasan a través de redes públicas debería ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.	**SI**	L3	Existen procedimientos se seguridad implantados. El acceso a la información es a través de logins et clave secreta, se tienen instalados firewalls et vpn's para el tunnelign de las conexiones.
14.1.3 Protecciones de las transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones debería ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.	**SI**	L3	Existen mecanismos de protección de transacciones implantados. Técnicas como el cifrado de los datos, protocolos para la transmisión segura (HTTPS), certificados de seguridad

14.2 Seguridad en el desarrollo y en los procesos de soporte	Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.		L3	
14.2.1 Política de desarrollo seguro	Se deberían establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	**SI**	L3	Se han definidos la política de desarrollo seguro de aplicaciones y sistemas. Ha sido aprobado y puesto en conocimiento del personal de desarrollo. Sin embargo no existe registro de la revisión regular de las políticas.
14.2.2 Procedimiento de control de cambios en el sistema	La implantación de cambios a lo largo del ciclo de vida del desarrollo debería controlarse mediante el uso de procedimientos formales de control de cambios.	**SI**	L3	Existen procedimientos formales definidos para la gestión de los cambios. Los cambios en los sistemas son revisados para verificar que no comprometen la seguridad del sistema o del entorno operativo. Sin embargo existe evidencia de que algunos cambios aprobados no tienen documentados las especificaciones de controles de seguridad necesarios.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deberían ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	**SI**	L3	Existen procedimientos definidos para la revisión del impacto de los cambios en la integridad de las aplicaciones. No existen evidencias de una revisión regular de los procedimientos definidos. Ni registros de pruebas y revisiones antes de la implantación de los cambios.
14.2.4 Restricciones a los cambios en los paquetes de software	Se deberían desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deberían ser objeto de un control riguroso.	**NO**	L2	Toda modificación sobre los paquetes de software pno asa por un proceso de revisión y aprobación. Los registros muestran que se realizan cambios no autorizados.
14.2.5 Principios de ingeniería de sistemas seguros	Principios de ingeniería de sistemas seguros se deberían establecer, documentar, mantener y aplicarse a todos los esfuerzos de implantación de sistemas de información.	**NO**	L3	Se han definidos principios y procedimientos de ingeniera de sistemas de información seguros. Estos están documentados y publicados para su aplicación. Sin embargo, no existe registro de revisiones recientes de estos principios.
14.2.6 Entorno de desarrollo seguro	Las organizaciones deberían establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	**NO**	L3	Los entornos de desarrollo están segregados y protegidos y solo tienen acceso los desarrolladores. Sin embargo existe registro de acceso a los entornos de desarrollo por personal no desarrollador.
14.2.7 Externalización del desarrollo de software	El desarrollo de software externalizado debería ser supervisado y controlado por la organización.	**SI**	L3	Existen procedimientos definidos para la supervisión y el control de desarrollo de software externalizado. Sin emabrgo, no existe evidencia de revisiones recientes de estos procedimientos.
14.2.8 Pruebas funcionales de seguridad del sistema	Se deberían llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	**SI**	L3	Existen procedimientos definidos para realizar las pruebas funcionales. No existe registro de la realización de pruebas funcionales ejecutadas para todos los proyectos de desarrollo.
14.2.9 pruebas de aceptación del sistema	Se deberían establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	**SI**	L3	Existen procedimientos definidos y aprobados para la ejecución de pruebas de aceptación del sistema. Pero los registros no indican que se hayan revisado recientemente.
14.3 Datos de prueba	Asegurar la protección de los datos de prueba		L2	

14.3.1 Protección de los datos de prueba	Los datos de prueba se deberían seleccionar con cuidado y deberían ser protegidos y controlados.	**NO**	L3	Existen procedimientos definidos para la selección de los datos de prueba, su protección y su control. Sin embargo no existe evidencia de la revisión de los registros de las copias de datos de las bases de datos de la producción hacia las Bases de Datos de Tests.
15. RELACIONES CON PROVEEDORES			L3	
15.1 Seguridad en las relaciones con los proveedores	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		L3	
15.1.1 Política de seguridad de la información en las 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 deberían acordarse con el proveedor y quedar documentados.	**SI**	L3	Se implantan mecanismos de control de acceso a los dispositivos de tratamiento de información de la organización por parte de los proveedores. Existe un documento que define las políticas de acceso y los requisitos de seguridad de la información que requieren los activos de la. Sin embargo, no existe evidencia de la revisión de estas políticas o controles. Existen contratos con los proveedores en los que no se menciona estas políticas.
15.1.2 Requisitos de seguridad en contratos con terceros	Todos los requisitos relacionados con la seguridad de la información deberían establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.	**SI**	L3	Se establecen y se acuerdan con los proveedores los requisitos relacionados a la seguridad de la información. El respeto de los mismos está especificado en todos los contratos con los proveedores. Sin embargo en los acuerdos no existe mención que estos acuerdos deben ser respetados por los subcontratistas.
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	**SI**	L3	El acuerdo con los proveedores incluye los requisitos para abordar los riesgos de seguridad de la información relacionados a las TICS y con la cadena de suministro de los servicios. Se exige a los proveedores certificaciones iso27001. Sin embargo, existe evidencia que no todos los proveedores críticos poseen estas certificaciones.
15.2 gestión de la provisión de los servicios del proveedor	Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.		L3	
15.2.1 Control y revisión de la provisión de servicios del proveedor	Las organizaciones deberían controlar, revisar y auditar regularmente la provisión de servicios del proveedor.	**SI**	L3	SE realizan revisiones y controles de los niveles de servicios de proveedores. Estas evaluaciones y revisiones se realizan en reuniones con los proveedores. La empresa solicita auditorias a los proveedores. Existe un plan de revisiones definidos con los principales proveedores de servicios. .
15.2.2 Gestión de cambios en la provisiones del proveedor	Se deberían gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	**SI**	L3	Existe un procedimiento definido de control de cambios formalizado y que se encuentra en aplicación para todos los casos analizados. Existe una persona dedicada a la gestión de las relaciones con los proveedores . Sin embargo, existe evidencia de que algunos cambios no han sido documentados.
16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION			L3	

16.1 Gestión de incidentes de seguridad de la información y mejoras	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.		L3	
16.1.1 Responsabilidades y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	**SI**	L3	Existen procedimiento definidos para la gestión de incidentes de seguridad de la información. Se han comunicado los procedimientos y se han establecido responsables para su gestión. Sin embargo, se tiene registro de incidentes que no han sido tratados con la celeridad requerida.
16.1.2 Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible.	**SI**	L3	Los canales de notificación están definidos y comunicados al personal. Esta información esta disponible en el portal interno de la empresa.
16.1.3 Notificación de puntos débiles de la seguridad	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	**NO**	L2	La empresa dentro de la formación de la seguridad aborda el tema de la notificación inmediata de los incidentes. Busca concientizar a los trabajadores de la importancia de una notificación temprana. Sin embargo existe evidencia de notificaciones tardías debido a desconocimiento sobre la identificación de los puntos débiles. Las notificaciones no son inmediatas, el mecanismo de comunicación disponible no es conocido por los usuarios.
16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información deberían ser evaluados y debería decidirse si se clasifican como incidentes de seguridad de la información.	**SI**	L3	El punto de contacto evalúa y decide. Asimismo delega el tratamiento al equipo de respuesta cuando considere necesario. Se evidencia en los registros que existen incidentes cuyas evaluaciones no han sido documentados.
16.1.5 Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.	**SI**	L3	Existe un procedimiento definido de respuesta a los incidentes. Sin embargo se constata en registros que no todos los incidentes han sido comunicados a los interesados.
16.1.6 Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	**SI**	L3	Existe un plan anual de revisión de los principales incidentes de la empresa. Se busca sobre todo identificar nuevos controles. Se elabora un articulo sobre los incidentes importantes, las observaciones, recomendaciones y conclusiones. Este articulo es publicado en la revista en línea dentro del portal interno de la empresa.
16.1.7 Recopilación de evidencias	La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.	**SI**	L5	Existen procedimientos definidos y este proceso de recuperación de evidencias y la aplicación de procedimientos es externalizado.
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS			L3	
17.1 Continuidad de la seguridad de la información	La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de continuidad de negocio de la organización.		L3	

17.1.1 Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	**SI**	L3	La organización ha determinado que los requisitos de seguridad de la información en situaciones adversas. Estos se encuentran dentro del plan de continuidad de negocio y la recuperación de desastres.
17.1.2 Implementar la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	**SI**	L3	Existen procesos, procedimientos y controles para garantizar la continuidad de la seguridad de la información. Se ha creado una infraestructura de gestión que cuenta con la responsabilidad, autoridad y competencia para ello.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	**SI**	L3	Existe un plan de revisión anual de la validez y la efectividad del plan de continuidad del negocio. Se tienen programadas pruebas y simulaciones.
17.2 Redundancias	Asegurar la disponibilidad de los recursos de tratamiento de la información.		L3	
17.2.1 Disponibilidad de los recursos de tratamientos de la información	Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	**SI**	L3	La empresa cuenta con una infraestructura redundante. Esta infraestructura y su funcionamiento esta externalizado. Esta estructura esta implementada.
18. CUMPLIMIENTO			L3	
18.1 Cumplimiento de los requisitos legales y contractuales	Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.		L4	
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	**SI**	L3	Los principales sistemas de información definen y documentan los requisitos legales regulatorios
18.1.2 Derechos de propiedad intelectual	Deberían implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	**SI**	L3	Existe una guía de buena practicas a aplicar en la empresa para controlar el software que se utiliza y el uso de las licencias.
18.1.3 Protección de los registros de la organización	Los registros deberían estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	**SI**	L3	La información de los registros es almacenada y existe un mecanismo de control de acceso que busca evitar los accesos no autorizados.

18.1.4 Protección y privacidad de la información de carácter personal	Debería garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	**SI**	L3	Existe un documento que resume la política de privacidad y protección de la información de carácter personal. Este documento es de conocimiento del personal y forma parte del programa de la formación que han seguido los empleados de la empresa.
18.1.5 Regulación de los controles criptográficos	Los controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	**NO**	L3	Existe un documento que menciona sobre los controles criptográficos deseables implementar. Pero no existe un documento definido sobre las políticas de los controles criptográficos.
18.2 Revisiones de la seguridad de la información	Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.		L3	
18.2.1 Revisiones independientes de la seguridad de la información	El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debería someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	**SI**	L3	Existe un plan de auditorias que se realiza cada 3 años. Se encuentran registros de los resultados de la auditoria de hace 3 años.
18.2.2 Cumplimiento de las políticas y de las normas de seguridad	Los directivos deberían asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.	**SI**	L3	Existe un plan de revisión de los procedimientos de seguridad dentro de la empresa. Este plan se ejecuta cada anio, y es responsabilidad de la dirección.
18.2.3 Comprobación del cumplimiento técnico	Debería comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	**SI**	L3	Existe un plan de revisiones de cumplimiento técnico. Este plan se realiza cada tres años. Es realizado por expertos externos independientes.

ANEXO XVIII

INFORME DE AUDITORIA DE CUMPLIMIENTO

Nivel de Madurez CMM para las dominios de la norma ISO/IEC 27001:2013

Elaborado por: Ruth Aguilar

junio 2017

Contenido

AUDITORIA DE CUMPLIMIENTO

I RESUMEN EJECUTIVO

Alcance

Auditoría del Sistema de Gestión de la Seguridad de la empresa dentro de los limites del alcance del SGSI y de la declaración de aplicabilidad de los diferentes controles.

Objetivo

Evaluar la madurez de la Seguridad en lo que respecta a los diferentes dominios de control los 114 controles planteados por la ISO/IEC 27002:2013.

Metodología

El proceso de auditoría de cumplimiento se la ha realizado mediante una evaluación al cumplimiento de cada uno de los controles de la norma ISO / IEC 27002: 2013, para ello se ha utilizando el Modelo de Madurez de la Capacidad (CMM). Esta evaluación de control se la ha realizado mediante un análisis de los recursos que se disponen: documentación existente dentro de la empresa, reportes de evidencias, reportes de incidentes, reportes de funcionamiento de la empresa, de reportes de evaluaciones, reportes de auditorias precedentes, reportes de entrevistas, de tests y observaciones realizadas en situ.

Principales conclusiones

El nivel de madurez no es el optimizado y existen todavía inconformidades. Los resultados obtenidos en los diferentes dominios muestran que la empresa es consiente de la importancia de la seguridad de la información y para ello ha implementado medidas tanto funcionales como técnicas que permitan mejorar el manejo seguro de la información.

La auditoria ha permitido identificar 19 no conformidades de las cuales 3 conformidades mayores. Resultado de estos hallazgos se constata que existen deficiencias mayores en las medidas que se han tomado para controlar los accesos a la información y a los recursos de manejo de la información.

Se han identificado que existen deficiencias en la concientización de los usuarios afectando de manera directa el nivel de seguridad del manejo de la información.

Recomendaciones

Es necesario tomar acciones inmediatas para subsanar primero las no conformidades mayores planificando la conclusión de la mismas en un periodo de tiempo corto, lo que permitiría mejorar el nivel de la seguridad en un plazo corto. Si bien no existe un plazo limite para tomar acciones para subsanar las no

conformidades menores, es recomendable una planificación inmediata de ejecución de las mismas.

II METODOLOGIA

El proceso de auditoría de cumplimiento se la ha realizado mediante una evaluación al cumplimiento de cada uno de los controles de la norma ISO / IEC 27002: 2013, para ello se ha utilizando el Modelo de Madurez de la Capacidad (CMM).

Fases de la Auditoria

Fase 1: Recolección de la Información

Durante esta etapa se ha solicitado toda la documentación relevante al proceso de auditoria. documentación que permite entender el entorno del ambiente a auditar, las políticas, los procedimientos definidos, los procesos implementados, los registros e informes y evaluaciones precedentes, etc.
Es en esta etapa que se realiza la identificación y la asignación de recursos.

Fase 2. Ejecución de pruebas documentadas

Revisión de la documentación que se ha recopilado con el fin de comprobar la idoneidad y relevancia con el proceso de auditoria que se lleva a cabo.
Se han revisado y validado el estado de implementación de los procedimientos y procesos Asociados al manejo de la información y los sistemas de información.

Se verifica la implementación de los distintos controles estipulados en la declaración de la aplicabilidad.

Se han procedido a entrevistas para comprobar si el personal de la empresa conoce las políticas, procesos y procedimientos y las aplica.

Se han realizado visitas para examinar aspectos de seguridad y comprobar en situ el modo en el que maneja la información y se operan los sistemas de información.

Fase3: Análisis de la información

Se ha analizado toda la documentación disponible y las evidencias que se han recolectado para poder determinar el nivel de cumplimiento con la norma.

Esta fase se ha enfocado por un lado en la revisión de las políticas, para verificar que se encuentran al alcance del personal, que son claras, relevantes, que protegen los activos identificados, que se conocen a los responsables de emitir estas políticas y a quienes afectan las mismas. Po otro lado se enfoca en el análisis de los resultados de las entrevistas, de las verificaciones y observaciones que se han realizado en situ y así poder evaluar si las políticas se distribuyen, se comunican y se aplican. Es a partir de este análisis que se puede concluir la efectividad de los controles implementados.

Como resultado de esta fase se han identificado los incumplimientos a la norma y muestra la eficiencia y la efectividad de los controles de seguridad.

Fase 4: Elaboración y presentación del Reporte de la Auditoria

Se elabora el informe de auditoría que transmite las conclusiones a las que se han llegado.

III HALLAZGOS y RECOMENDACIONES

Puntos Fuertes

- COMPROMISO POR PARTE DE LA DIRECCION

Se constata que la Dirección esta realmente comprometida con la implementación del PLAN. Este compromiso queda reflejado en la creación del Comité de Seguridad encabezado por el Director General con un plan de revisiones anuales para los próximos 3 años.

- POLITICAS BIEN DEFINIDAS Y APROBADAS

El documento de las políticas están definidas y aprobadas por la dirección. De igual manera se han dado los instructivos provenientes de la dirección para que estos sean comunicados a todo el personal y socios comerciales de la empresa. De igual manera existe un plan de revisión anual definido y aprobado por la dirección.

Oportunidades de mejora

- FORMACION/CONCIENTIZACION

Si bien la empresa tiene planificado un plan de formación que involucra a todo el personal y socios comerciales.
Este plan de formación es obligatorio por lo menos una vez y cada vez que el usuario cambia de puesto de trabajo.

Se han identificado en algunos miembros del personal cierta desactualización en algunos temas relacionado al manejo de la seguridad. Es por eso que se plantea que el personal del la empresa debería pasar por el proceso de concientización/formación por lo menos una vez al año. Para dar mayor flexibilidad y accesibilidad a la formación se podría considerar implementar una metodología de e-learning.

No Conformidades

ID: NC-001	**Fecha:** 20/05/2017
Descripción NC	
El tratamiento de la seguridad de la información dentro de los proyectos depende de	

la iniciativa de los responsables de proyectos.	
Tipo	
Referencia normativa	
Controles	**Dominio**
6.1.5 Seguridad de la información en la gestión de proyectos	6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
Acción Correctora	
Definir una directiva clara que especifique que la seguridad debe ser tratada dentro la gestión de proyectos. Esta directiva tiene que estar aprobada por la dirección.	
Responsable Ejecución acción correctora	
El responsable de la seguridad con aprobación de la Dirección	

ID: NC-002	**Fecha:**	20/05/2017
Descripción NC		
- Existen registros de un numero importante de incidentes de seguridad en los dispositivos móviles. - Existen registros de un numero importante de incidentes de Seguridad durante el teletrabajo.		
Tipo	**☐ Mayor**	**☑ Menor**
Referencia normativa		
Controles		**Dominio**
6.3.1 Política de uso de dispositivos para movilidad. 6.1.2 Teletrabajo		6.2 Dispositivos para movilidad y teletrabajo
Acción Correctora		
-Organizar sesiones de formación y concientización sobre la seguridad de la información y los riesgos en general y en particular en lo que se refiere a los dispositivos móviles y el teletrabajo. - Cada empleado que utilice un dispositivo móvil y/o trabaje a distancia debe pasar esta formación/sesión antes de usar un dispositivo móvil o comenzar el teletrabajo. -Cada empleado debe firmar un documento de responsabilidad.		
Responsable Ejecución acción correctora		
Responsable de Recursos Humanos – Responsable de la Seguridad		

ID: NC-003	**Fecha:**	20/05/2017
Descripción NC		
Existen todavía algunas aplicaciones donde la información secreta no es manejada		

completamente por los usuarios y no sigue los procesos formales definidos para ello. No existe registro de los usuarios que tienen acceso a las cuentas privilegiadas.
☑ **Mayor** ☐ **Menor**
Referencia normativa: ISO/IEC 27002:2013

Controles	**Dominio**
9.2.4 Gestión de la información secreta de autenticación de los usuarios	9.2 Gestión de acceso de usuario

Acción Correctora
Implementar un proceso formal de asignación de claves secretas para todas las aplicaciones faltantes. Responsabilizar al usuario de la confidencialidad de las información secreta.
Responsable Ejecución acción correctora
Responsable IT, Responsable de la Seguridad

ID: NC-004	**Fecha:**	20/05/2017
Descripción		
El procedimiento seguro de inicio de sesión no esta implantado en todos las aplicaciones que lo requieren. Los sistemas de gestión de contraseñas no están implementados en todos los sistemas ni en todas las aplicaciones. Existen diferentes sistemas de gestión de contraseña implementados.		
Tipo	☑ **Mayor**	☐ **Menor**
Afectación ISO/IEC 27002:2014		

Controles	**Dominio**
9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Sistema de gestión de contraseñas	9.4 Control de acceso a sistemas y aplicaciones

Acción Correctora
Planificar e implantar el procedimiento seguro de inicio de sesión y los sistemas de gestión de contraseñas en los sistemas y las aplicaciones faltantes.
Responsable acción correctora
Responsable IT

ID: NC-005	**Fecha:**	20/05/2017
Descripción		

La política esta definida dentro de las políticas de seguridad de la empresa. No existe registro de uso o de difusión de esta política. No existe registro de una revisión en los últimos 3 años de la política.

Tipo	☐ **Mayor**	☑ **Menor**

Afectación ISO/IEC 27002:2014

Controles	**Dominio**
10.1.1 Política de uso de los controles criptográficos	10. CRIPTOGRAFIA

Acción Correctora

Organizar sesiones de información/concientización de la política.
Designar responsables de la aplicación de esta política.

Responsable acción correctora

Responsable de la seguridad – Responsable recursos humanos

ID: NC-006	**Fecha:**	20/05/2017

Descripción

Existe evidencia de malas practicas por parte de los usuarios. Muchos usuarios tienen sus aplicaciones activas y abiertas aun cuando éstas no están siendo utilizadas.

La política de clean & clean desk existe y ha sido comunicada a todos los empleados. Sin embargo, existe evidencia de resistencia a la aplicación de estas políticas por un numero considerable de usuarios.

Tipo	☐ **Mayor**	☑ **Menor**

Afectación ISO/IEC 27002:2014

Controles	**Dominio**
11.2.8 Equipo de usuario desatendido 11.2.9 Política de puesto de trabajo despejado y pantalla limpia	11.2 Seguridad de los equipos

Acción Correctora

Organizar sesiones de información/concientización sobre las políticas de seguridad y sus consecuencias de la no aplicación.

Responsabilizar y aplicar procesos disciplinarios a los infractores.

Responsable acción correctora

Responsable de la seguridad, Responsable Recursos humanos

ID: NC-007	Fecha:	20/05/2017
Descripción		
Se evidencia de cambios realizados sin haber pasado por el procedimiento formal. No existe un plan documentado de gestión de la capacidad de los recursos. No existe evidencia de una revisión reciente de las actividades de administrador, ni un informe sobre el registro de actividades de los administradores del año pasado.		
Tipo	☐ **Mayor**	☑ **Menor**
Afectación ISO/IEC 27002:2014		
Controles	**Dominio**	
12.1.2 Gestión de cambios 12.1.3 Gestión de capacidades 12.4.3 Registros de administración y operación	12.4 Registros y supervisión	
Acción Correctora		
Aplicar los procedimientos formales de la gestión de cambio y asignar responsabilidades Elaborar un plan documentado de la capacidad de recursos humanos por lo menos una vez al año. Se deben planificar las revisiones de las actividades del administrador y los operadores por lo menos una vez al año. Se debe asignar un responsable del proceso de revisión.		
Responsable acción correctora		
Responsable de la seguridad, Responsable IT, Responsable Operations		

ID: NC-008	Fecha:	20/05/2017
Descripción		
Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes no siempre especifican los requisitos relacionados a la seguridad de la información en las etapas iniciales.		
Tipo	☐ **Mayor**	☑ **Menor**
Afectación ISO/IEC 27002:2014		
Controles	**Dominio**	

14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	14. Adquisición, desarrollo y mantenimiento de los sistemas de información

Acción Correctora

Por cada nuevo sistema de información o intervención de mejora, se debe presentar un análisis de los requisitos de seguridad a gestionar en el proyecto y sus procesos asociados.

Responsable acción correctora

Responsable IT y Responsable de la seguridad

ID: NC-009	**Fecha:**	20/05/2017

Descripción

Toda modificación sobre los paquetes de software no pasa por un proceso de revisión y aprobación. Los registros muestran que se realizan cambios no autorizados.

Se han definidos principios y procedimientos de ingeniera de sistemas de información seguros. Estos están documentados y publicados para su aplicación. Sin embargo, no existe registro de revisiones recientes de estos principios.

Los entornos de desarrollo están segregados y protegidos y solo tienen acceso los desarrolladores. Sin embargo existe registro de acceso a los entornos de desarrollo por personal no desarrollador.

Existen procedimientos definidos para la selección de los datos de prueba, su protección y su control. Sin embargo no existe evidencia de la revisión de los registros de las copias de datos de las bases de datos de la producción hacia las Bases de Datos de Tests.

Tipo	**☐ Mayor**	**☑ Menor**

Afectación ISO/IEC 27002:2014

Controles	**Dominio**
14.2.4 Restricciones a los cambios en los paquetes de software 14.2.5 Principios de ingeniería de sistemas seguros 14.2.6 Entorno de desarrollo seguro 14.3.1 Protección de los datos de prueba	14. Adquisición, desarrollo y mantenimiento de los sistemas de información

Acción Correctora

Todo cambio en el paquete de software debe ser aprobado antes de instalarse. Se debe asignar un responsable de este proceso.

Planificar la revisión de los principios de ingeniería y asignar un responsable para la

revisión y la aplicación. Se deben hacer revisiones de los accesos para identificar estas violaciones, las causas y aplicar las soluciones y/o sanciones. Toda copia de datos de la producción debe ser revisada y debe emitirse un informe sobre esta revisión. Asignar un responsable a esta tarea.
Responsable acción correctora
IT, Responsable de la Seguridad, Responsable de Recursos humanos

ID: NC-010		20/05/2017
Descripción		
Las notificaciones no son inmediatas, el mecanismo de comunicación disponible no es conocido por los usuarios.		
Tipo	☐ **Mayor**	☑ **Menor**
Afectación ISO/IEC 27002:2014		
Controles	**Dominio**	
16.1.3 Notificación de puntos débiles de la seguridad	16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION	
Acción Correctora		
Realizar una encuesta para identificar las razones por las cuales las comunicaciones no son inmediatas. Identificar los problemas en el mecanismo de comunicación disponible. Organizar un mini training en el mecanismo de comunicación.		
Responsable acción correctora		
Responsable de RH, Responsable IT		

ID: NC-011	**Fecha:**	20/05/2017
Descripción		
No existe un documento definido sobre las políticas de los controles criptográficos.		
Tipo	☐ **Mayor**	☑ **Menor**
Afectación ISO/IEC 27002:2014		
Controles	**Dominio**	
18.1.5 Regulación de los controles criptográficos	18. CUMPLIMIENTO	

Acción Correctora
Elaborar un documento que defina las políticas sobre los controles criptográficos con miras a cumplir con los acuerdos, la legislación y la reglamentación aplicables.
Responsable acción correctora
Responsable de la Seguridad

IV CONCLUSIONES

Los resultados confirman que la empresa en su conjunto participa en la implementación de los controles necesarios para garantizar un manejo seguro de la información. Si bien no se ha llegado al nivel optimizado y existen todavía no conformidades mayores, los resultados obtenidos en los diferentes dominios muestran que la empresa es consiente de la importancia de la seguridad de la información y para ello ha implementado medidas tanto funcionales como técnicas que permiten mejorar el manejo seguro de la información.

El resultado de la evaluación del nivel de madurez de seguridad de la información en la empresa es satisfactorio puesto que la mayoría de procesos y controles se encuentran adecuadamente en el nivel de “Definido”.

Los resultados de muestran que a través de la implementación de este plan director se están consiguiendo mejoras en los diferentes dominios de la norma de referencia.

BIBLIOGRAFÍA

- MATERIAL UOC

  Asignatura Sistemas de Gestión de la Seguridad

  Modulo1: Introducción a la Seguridad de la Información
  Modulo2: Análisis de riesgos
  Modulo 3: Implantación de un Sistema de Gestión de la Seguridad de la Información
  Modulo 4: Desarrollo de Algunos Objetivos de control del SGSI

  Asignatura de la Auditoria

  Modulo 2: Auditoria de Certificación

- MAGERIT: metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica Actualizada en 2012 en su versión 3
  http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- ISO 27001: Revisión por la dirección y mejora del SGSI
  http://www.pmg-ssi.com/2014/12/iso-27001-revision-por-la-direccion-y-mejora-del-sgsi/

- ¿Qué es el Capability Maturity Model (CMM®)?
  http://www.pmvalue.com.ar/newsletters/Newsletter%20-%20CMM.pdf