Master Interuniversitario en Seguridad de las TIC

DESARROLLO DE UN PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACION PARA LA IMPLEMENTACIÓN DE UN SGSI

TRABAJO FINAL DE MÁSTER

AUTOR: Freddy Vinicio Jara C.

TUTOR: Antonio José Segovia H.

Junio, 2019

RESUMEN

El presente TFM, tiene como objeto desarrollar el Plan Director de la seguridad de la información de una empresa, basado en el estándar internacional ISO/IEC 27001:2013 certificable y el manual de buenas prácticas ISO/IEC 27002 :2013 que describe los controles o salvaguardias para mitigar las amenazas.

La implementación de un SGSI y mediante la metodología de análisis de riesgo MAGERIT, ha permitido a la empresa realizar un inventario de sus activos y valorarlos en las dimensiones de seguridad, así como identificar las amenazas que se podrían materializar en los activos. Calcular el impacto potencial y medir el nivel de riesgo de los activos, para posteriormente realizar una propuesta de proyectos, que tiene la finalidad de mejorar el nivel de cumplimiento de los estándares ISO/IEC 27001-27002. Finalizando con una auditoria de cumplimiento usando el modelo de madurez de la capacidad (CMM).

PALABRAS CLAVE

ISO/IEC 27001, ISO/IEC 27002, SGSI, Plan director de Seguridad, seguridad de la información, seguridad informática, Análisis de riesgo, gestión de riesgos, MAGERIT.

ABSTRACT

The purpose of this TFM is to develop the Master Plan for information security of a company, based on the ISO / IEC 27001: 2013 international certifiable standard and also based on the ISO / IEC 27002: 2013 good practices manual that describes the controls or safeguards to mitigate the threats.

The implementation of an SGSI using the MAGERIT risk analysis methodology has allowed to the company to carry out an inventory of its assets and value them in the security dimensions, as well as identify the threats that could materialize in the assets. Calculate the potential impact and measure the level of risk of the assets, to subsequently make a project proposal, which aims to improve the level of compliance with ISO / IEC 27001-27002 standards. Finalizing with a compliance audit using the Capability Maturity Model CMM

KEYWORDS

ISO / IEC 27001, ISO / IEC 27002, ISMS, Master Plan for Security, Information Security, IT Security, Risk Analysis, Risk Management, Magerit.

ÍNDICE DE CONTENIDOS

LISTADO DE FIGURAS

LISTADO DE TABLAS

1. INTRODUCCIÓN

El presente Trabajo Final de Master (TFM) tiene como objeto establecer las bases para la realización del Plan Director de Seguridad de la Información de una empresa, el mismo que le permitirá alinear sus objetivos y principios de seguridad, a la normativa internacional de referencia ISO/IEC 27001:2013 – 27002:2013, como primer paso se obtendrá información del estado actual, del nivel de seguridad de la información para poder plantear acciones pertinentes para mitigar amenazas y riesgos que se presentan en los activos de información de la empresa, protegiendo los tres pilares bases de la seguridad como son la integridad, confidencialidad y disponibilidad de la información.

Para poder cumplir con este proyecto se dividirá en 6 fases:

- **Fase 1: Introducción al Proyecto,** aquí se definirán los objetivos del Plan Director de Seguridad y se realizará un análisis diferencial de la compañía con respecto a la norma ISO/IEC 27001 - ISO/IEC 27002.
- **Fase 2: Sistema de gestión documental,** donde se elaborarán las políticas de seguridad, declaración de aplicabilidad y documentación del SGSI.
- **Fase 3: Análisis de riesgos**, identificación y valoración de activos, análisis de amenazas y vulnerabilidades, cálculo de nivel de riesgo aceptable y residual, donde se obtendrá un conjunto de medidas que garantizarán la funcionalidad de los activos y recordando que estas medidas no pueden tener un valor económico mayor al activo protegido.
- **Fase 4: Propuesta de proyectos,** con fines de mejoramiento que permiten enfrentar a las vulnerabilidades y amenazas encontradas en los activos, constituyéndose como salvaguardas a corto, mediano y largo plazo para la continuidad del negocio. Cabe recalcar que estas propuestas no solo son en el ámbito tecnológico sino también deben incluir diferentes ámbitos como son los recursos humanos y de organización
- **Fase 5. Auditoría de cumplimiento**, evaluación de controles y madurez, está es una fase crucial para poder evidenciar el nivel de cumplimiento de todas las salvaguardas aplicadas, para poder cumplir con la protección integral de la seguridad de la información. La evaluación de la madurez es con respecto a los dominios, objetivos y controles de la ISO/IEC 27002:2013. Esta

estimación se la realizará en una tabla basada en el Modelo de Madurez de la Capacidad (CMM). Y para finalizar:

- **Fase 6. Presentación de resultados y entrega de Informes,** es donde se consolidan los resultados obtenidos durante el proceso de análisis, y se le da un formato de presentación que incluye un resumen ejecutivo, memoria global del proyecto y una presentación a los directivos con los principales resultados de estudio.

2. GLOSARIO DE TERMINOS

- **Activo:** son todos aquellos elementos que posee la organización y que serán analizados durante el proceso (sistemas, soportes, edificios, personas..)y que requiere la organización para poder realizar las actividades de negocio que le son propias.
- **Aceptación del riesgo:** Esta decisión consiste en que la organización ha detectado que se encuentra expuesta a un riesgo importante y su probabilidad de que llegue a suceder es tan improbable, que no resulta posible la inversión para protegerse ante esta situación. La decisión es que la organización trabaje aceptando que está expuesta al riesgo y, llegado el caso de que se produzca un incidente, improvisando una respuesta.
- **Alcance**: Ámbito de la organización que queda sometido al SGSI.
- **Amenaza:** son todas aquellas situaciones que podrían llegar a suceder en una organización y que podrían dañar a los activos, provocando que éstos no funcionen correctamente o que no puedan utilizarse del modo correcto para poder llevar a cabo la actividad de negocio de la organización
- **Análisis de riesgos:** proceso que permite descubrir qué necesidades de seguridad tiene la organización tras detectar cuáles son nuestros agujeros en seguridad, así como las amenazas a las que nos encontramos expuestos.
- **Compromiso de la dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.
- **Control:** o salvaguardia, práctica, procedimiento o mecanismo que reduce el nivel de riesgo.
- **CID:** Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.
- **Declaración de aplicabilidad:** Documento que recoge la relación de controles de la ISO 27002, especificando, para cada uno de ellos, si es o no de aplicación a la organización, junto con la justificación de su

aplicabilidad, o una descripción de cómo se implementa en caso de serlo. Este documento también se conoce como State of Aplicability (SOA).

- **Directiva o directriz:** Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Entidad de acreditación:** Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina), etc.
- **Entidad de normalización:** Un organismo oficial que genera y publica normas. Suele haber una por país. Son ejemplos de entidades de normalización: AENOR (España), BSI (Reino Unido), DGN (México), IRAM (Argentina), etc**.**
- **Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable**.**
- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **IEC:** International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas**.**
- **Impacto:** El coste para la empresa de un incidente -de la escala que sea, que puede o no ser medido en términos estrictamente financieros, ejemplo pérdida de reputación, implicaciones legales, etc.
- **Incidente de la seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** la información y sus métodos de procesamiento son exactos y completos, y no pueden ser manipulados sin autorización.
- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
- **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI).

- **ISO/IEC 27002:** Código de buenas prácticas en gestión de la seguridad de la información.
- **JTC1:** Joint Technical Committee. Comité técnico conjunto de ISO e IEC específico para las tecnologías de la información.
- **No conformidad:** Incumplimiento de un requisito.
- **No repudio:** Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Riesgo residual:** Es el estudio que se realiza teniendo en consideración las medidas de seguridad que la organización ya tiene implantadas. Como resultado de este proceso se obtiene un riesgo real.
- **Tratamiento del riesgo:** Proceso de modificar el riesgo, mediante la implementación de controles.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

3. CONTEXTUALIZACIÓN Y JUSTIFICACIÓN

Desde el momento que la empresa genera información, y se decide almacenarla, ya sea en medios físicos o virtualizados, pudiendo acceder a ellos de manera local o remota respectivamente, desde ese preciso instante necesitamos proteger la información.
La confidencialidad, integridad y disponibilidad de la información se ve comprometida día a día, en la actualidad existen diversas amenazas que aprovechan las vulnerabilidades del hardware y software. No siendo estos últimos solo los afectados, sino también las personas que, mediante técnicas de ingeniería social, son engañados con la finalidad de obtener información para poder realizar actos punibles o simplemente por demostrar sus habilidades en el campo informático.

El Código Orgánico Integral Penal (COIP) del Ecuador reconoce como delitos informáticos a la intercepción de comunicaciones, fraudes informáticos, revelación ilegal de información de bases de datos, ataque a la integridad de los sistemas informáticos, entre otros. (Policia Nacional del Ecuador, 2017).

En busca de soluciones a estos tipos de amenazas, nace la necesidad de la seguridad de la información, donde empresas del Ecuador y el mundo optan por invertir en la ciberseguridad. Un claro ejemplo es el Reglamento General de Protección de Datos (RGPD), que ha sido aprobado por el parlamento de la Unión Europea, mismo que persigue fortalecer los derechos de las personas en la protección de sus datos. (Advisiera, S/A)

La información y los sistemas que gestionan y guardan los datos, son considerados como los activos críticos de una empresa, debiendo invertir en recursos humanos capacitados, para gestionar la seguridad de sus datos. Corroborando la necesidad de la implementación de un SGSI que, permita resguardar su bien más importante como es la información.

Implantar un Sistema de Gestión de Seguridad de Información permitirá a la empresa:

- Registrar bases de proceso de mejora continua en materia de seguridad de la información.
- Conocer el estado actual de seguridad de la información y plantear acciones necesarias para minimizar el impacto de amenazas y riesgos potenciales.
- Analizar todos los activos involucrados en la gestión de información vital de la empresa.
- Mejorar algunos aspectos de la seguridad de la información existentes en la empresa.

4. CONCIENDO LA ISO 27000

En la actualidad un gran porcentaje de las empresas, entienden sobre el cuidado que deben tener sobre la información que ellas generan, no importa donde las tengan almacenadas, ya sea en un formato físico o digital. Por tal motivo buscan alguna manera para poder gestionar la seguridad de la información, implementando controles de acceso, firewalls, seguridad en sus redes inalámbricas, etc. Pero de manera arbitraria, sin antes de haber realizado un análisis de cuáles son sus principales debilidades.

Debido a estas necesidades existe la familia ISO 27000, siendo la 27001 y 27002 las que actualmente tienen mayor difusión y aceptación a nivel internacional.

El desarrollo de un SGSI se basa principalmente en las siguientes normativas:

4.1 ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. También permite que una empresa sea certificada; permitiendo que una entidad de certificación independiente pueda confirmar que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (Advisiera, S/A)

4.2 ISO 27002

La ISO 27002. Es el código de buenas prácticas para la gestión de la seguridad de la información. Tiene su origen en la BS 7799 parte 1 y la ISO / IEC 17799.
Realizando una síntesis sobre la ISO 27002, este estándar se puede utilizar como una guía práctica para desarrollar estándares de seguridad organizativa y prácticas efectivas de gestión de la seguridad, y puede ayudar a crear confianza en las relaciones con terceras organizaciones. (Cruz, Garre, Segovia, & Tortajada, 2018)
La ISO/IEC 27002:2013 presenta 14 dominios, 35 objetivos de seguridad y 114 controles. Que serán aplicados en la primera fase de este proyecto para obtener la situación actual de la compañía y realizar un análisis diferencial GAP.
La ISO en estudio, tal y como su título indica, es una guía de buenas prácticas. Pero no se debe considerar como una norma que se debe seguir al pie de la letra, sobre todo en lo que a las pautas de la guía de implantación se refiere, puesto que no todas ellas tienen por qué ponerse en práctica ni tampoco tienen por qué ser todas ellas aplicables a la situación concreta de la organización.
Por otra parte, es necesario recalcar que este estándar no es certificable, como sí lo es la ISO/IEC 27001. (Cruz, Garre, Segovia, & Tortajada, 2018).

4.3 MAGERIT

Con respecto a la metodología de gestión de riesgos que se usará es Magerit, que tiene las siguientes características principales:

- Esta metodología tiene como característica fundamental que los riesgos que se plantean para una organización se expresan en valores económicos directamente.
- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.
- El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta sea realmente costosa. (administracionelectronica.gob.es, 2012)

4.4 Comparativa ISO 9001 – ISO 27001

Según (Escuela Europea de Excelencia, 2016) las empresas que ya han implementado la norma ISO 9001 y desea implementar la norma ISO 27001, o piensa utilizar ambas normas a la vez, el mejor enfoque es crear un Sistema de Gestión integrado (SGI). Este Sistema de Gestión Integrado cumplirá con los requisitos de ambas normas. Ahorrando una gran cantidad de tiempo en la ejecución. Disminuyendo el esfuerzo de mantener el sistema y lograr el cumplimiento continuo con ambos estándares.

Los capítulos del SGC y del SGSI relacionados con el concepto de riesgo de gestión son los mismos, como se puede ver a continuación:

- **Contexto de la Organización**. Ambas normas requieren la identificación de los problemas internos y externos a la empresa, pero desde diferentes perspectivas. ISO 9001 se centra en la calidad e ISO 27001 se centra en la seguridad de la información.
- **Partes interesadas y requisitos**. La organización tendrá que determinar las partes interesadas y los requisitos relacionados con la calidad y seguridad de la información. Estos requisitos pueden ser abordados con el mismo proceso. Es buena idea crear una lista integrada de las partes interesadas.
- **Responsabilidad y autoridad para ser identificados**. Los roles y responsabilidades dentro del SGC y del SGSI son diferentes, pero de nuevo, deben ser definidos. Esto se puede llevar a cabo de la misma manera
- **Competencia, sensibilización, comunicación, control del sistema de documentos y registros.** Todos estos requisitos son comunes no sólo por la norma ISO 9001 e ISO 27001, sino para otras normas también. Por tanto pueden abordarse de la misma manera y al mismo tiempo.

- **Auditoría interna y revisión de la dirección.** Por supuesto, los requisitos para ser auditados y las entradas y salidas de revisión son diferentes. Pero la forma en que se lleva a cabo el proceso es la misma. Dependiendo del tamaño y la complejidad de la empresa y sus procesos, la auditoría interna o revisión de la dirección se pueden hacer al mismo tiempo o por separado.
- **Ambos requieren sistemas para acciones correctivas y de no conformidad.** El proceso de tratamiento de las no conformidades y acciones correctivas puede ser el mismo para ambos estándares. No hay ninguna razón aparente para separarlos.

5. SITUACIÓN ACTUAL

5.1 DESCRIPCIÓN DE LA EMPRESA

La empresa a la cual se le va implantar el Plan director de la seguridad de la información, es una compañía que se dedica al envasado y comercialización de gas licuado de petróleo (GLP), ubicada en el austro del Ecuador. La empresa tiene implementado un Sistema de Gestión de Calidad basado en la norma ISO/IEC 9001:2015 y se encuentra aprobado por la alta dirección.

Sus instalaciones tienen ubicaciones diferentes, la primera funciona el centro de acopio de GLP, y la segunda la planta envasadora. En el centro de acopio aproximadamente trabajan 50 empleados, divididos en diferentes unidades como son, Gerencia, Talento Humano, Legal, Financiero, Adquisiciones, Comercialización, Operaciones, S.I.G y TICs. En la planta envasadora aproximadamente existen 20 personas laborando, distribuidas en las unidades anteriormente descritas y se añade la unidad de transporte y logística.

Como se observa en el organigrama (Figura 1), la unidad de Tics tiene dependencia directa con Gerencia General y Subgerencia, siendo esta unidad la encargada de la responsabilidad de la seguridad de la información. Por la asignación de responsabilidades dentro de la compañía, debe haber una unidad independiente a las demás unidades que se encargue de la seguridad de la información con reporte directo a gerencia y directorio.

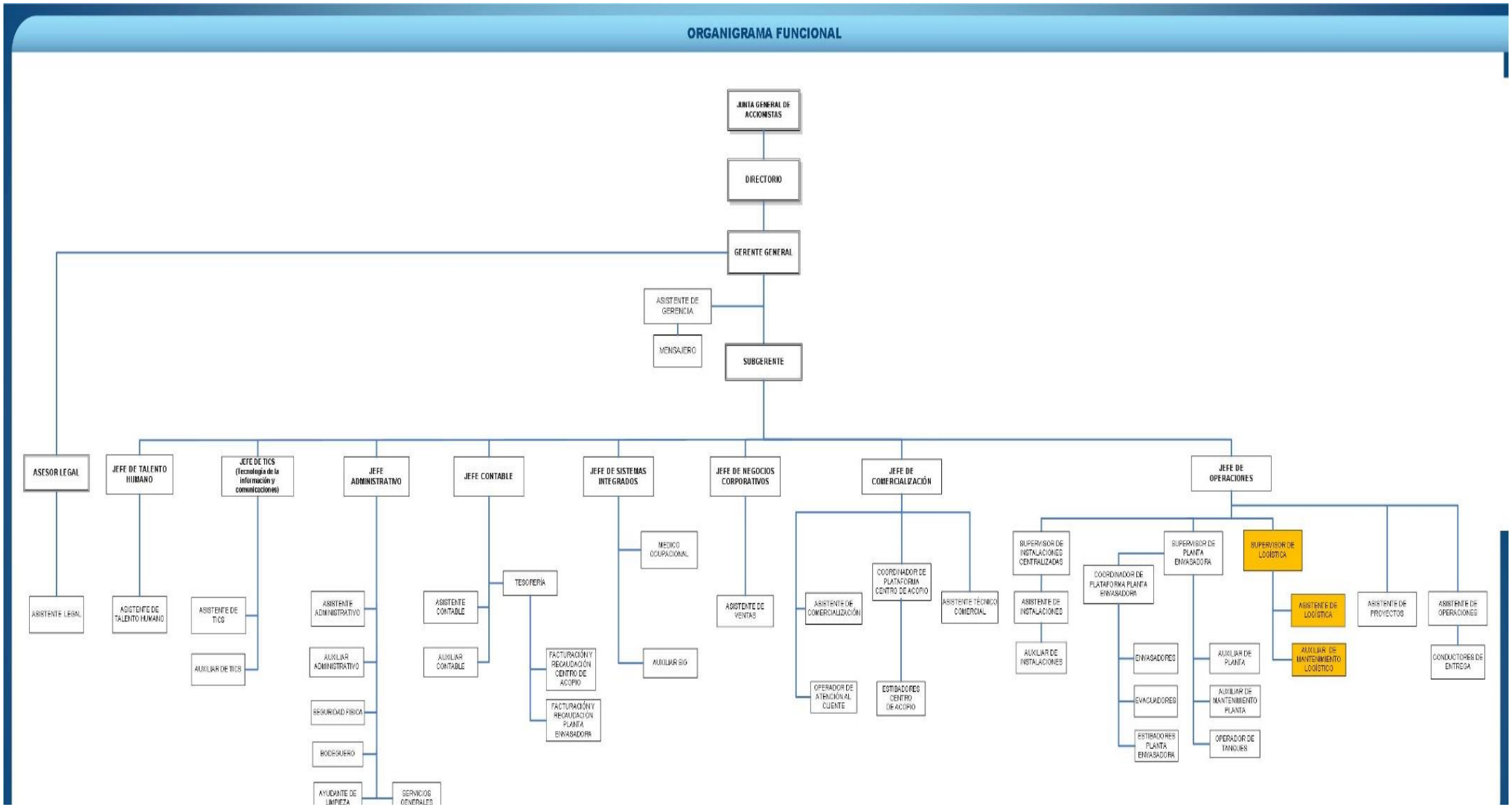


Figura 1. Orgánico funcional

El SGSI se enfocará exclusivamente en los procesos que tiene la unidad de TICs.

En cuanto al equipo de cómputo y telecomunicaciones, los enlaces entre diferentes infraestructuras es con fibra óptica, y el cableado estructurado se encuentra certificado con categoría 6. Casi en su totalidad los equipos de cómputos son con tecnología de última generación y debidamente licenciados.
Consta con seguridad 24 x 7 para el acceso a las instalaciones y sistemas de video vigilancia con detección de movimiento.
Los Centros de datos constan con puntos eléctricos debidamente regulados y con sistema de redundancia, bancos de baterías como sistema de respaldo eléctrico, sistemas de control de temperatura.

En cuanto al alcance de la organización con respecto a los sistemas de información, que permiten que la compañía pueda realizar sus actividades diarias, considerados como críticos y gestionados por la unidad de TICs son:

- Servicios públicos accesibles desde la red pública (Internet), pretendiendo que los clientes y empleados tengan acceso a los mismos sin la necesidad de entrar a la red interna.
- Servicios privados accesibles desde la red pública (Internet).
- Red Interna , específicamente a los CPD que cuentan con distintos servidores físicos y virtualizados tales como, bases de datos, ERP, sistema de facturación, consolas de gestión de seguridad de red, mesas de ayuda, servidores espejos, sistemas de video conferencia.

Se proporciona un diagrama lógico de red, al mismo que se pretende implementar un SGSI.(Figura 2).

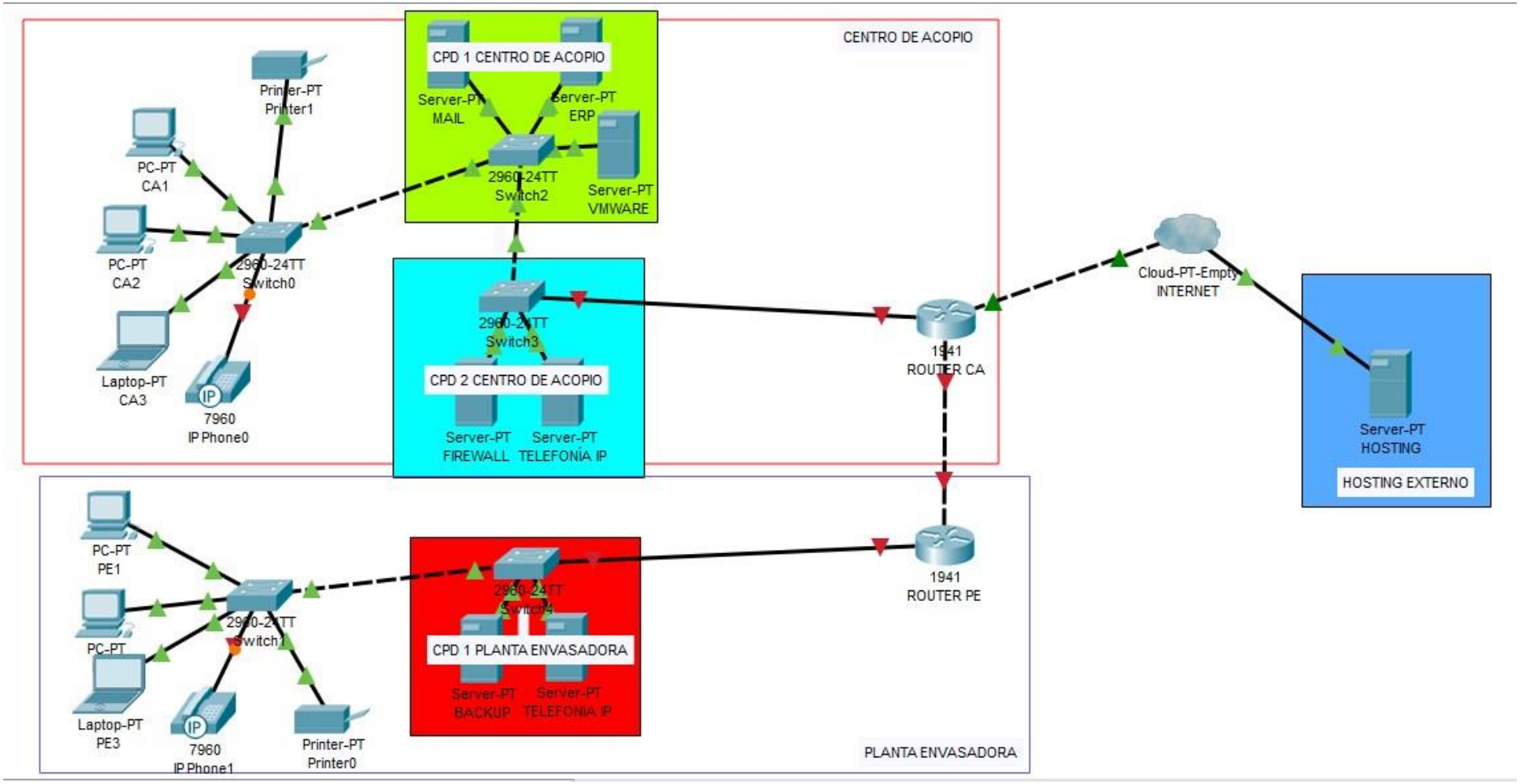


Figura 2. Diagrama lógico

5.2 OBJETIVOS DEL PLAN DIRECTOR

5.2.1 Objetivo General

El principal objetivo del presente proyecto es diseñar el plan director de seguridad e implementación de un SGSI para la empresa bajo estudio, que permita establecer las directrices y estándares ISO/IEC 27001-27002, como metodología de análisis y gestión de riesgos se usará MAGERIT.

5.2.2 Objetivos Específicos

- Asegurar la disponibilidad, confidencialidad e integridad de los activos de información críticos de la empresa.
- Reducir los riesgos a niveles aceptables en materia de la seguridad de la información a los que está expuesta la compañía.
- Definir y planificar los planes de acción a realizar a corto, mediano y largo plazo.
- Conocer y planificar las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado.
- Mejorar los niveles de seguridad de la información al fomentar una cultura de seguridad de la información en los empleados de la empresa.

5.2.3 Alcance

Este plan director de la seguridad de la información se direccionará en los procesos críticos gestionados por la unidad de TICs, aplicando estándares establecidos en la norma ISO/IEC 27001-27002:2013.
Describiendo el alcance sería:
La gestión de la seguridad de la información que cubra todas las actividades asociadas con los CPD de la empresa que dan soporte a los procesos críticos descritos en el literal 5.1, de acuerdo con la declaración de aplicabilidad.

5.2.4 Planificación del trabajo.

FASE	COMIENZO	FIN	Duración(semanas s, días d)
Situación actual: Contextualización, objetivos y análisis diferencial	08/03/2019	26/03/2019	2s 3d
Sistema de gestión documental	11/03/2019	22/03/2019	2s
Análisis de riesgos	25/03/2019	12/04/2019	3s
Propuestas de proyectos	15/04/2019	26/04/2019	2s
Auditoría de cumplimiento ISO/IEC 27002:2013	29/04/2019	17/05/2019	3s
Presentación de resultados y entrega de informes	20/05/2019	05/06/2019	2s 3 d

Tabla 1. Planificación del Trabajo

5.3 ANALISIS DIFERENCIAL

La compañía bajo estudio, no tiene implementado ningún SGSI, pero tiene algunas políticas establecidas, en la tabla 2, se muestra el resultado del análisis diferencial 27001:2013.

En la tabla 3, se muestra el análisis diferencial ISO/IEC 27002:2013, con la siguiente escala de calificación (Figura 3).

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

Figura 3. Escala de medición 27002, fuente WIKI UOC

Tabla 2. Análisis Diferencial 27001

REQUISITOS	COMENTARIOS	NIVEL DE CUMPLIMIENTO ISO/IEC 27001
4. CONTEXTO DE LA ORGANIZACIÓN		**40%**
4.1 Compresión de la organización y de su contexto	La compañía conoce los aspectos internos y externos que pueden afectar la capacidad de alcanzar los resultados previstos para su Sistema de Gestión de la Seguridad de la Información	50%
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Se comprende las necesidades y expectativas	50%
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información	Se tiene una idea sobre el alcance que tendrá el SGSI	60%
4.4 Sistema de gestión de la seguridad de la información	No hay un SGSI implementado, pero hay documentos que se han elaborado para poder gestionar la seguridad de la información	0%
5. LIDERAZGO		**50%**
5.1 Liderazgo y compromiso	La dirección se ha comprometido a dirigir y apoyar la eficacia del SGCI	90%
5.2 Política	Existen políticas pero no están aprobadas por la dirección, ni comunicadas al personal	60%
5.3 Roles, responsabilidades y autoridades en la organización	No cuenta con un comité de seguridad	0%
6. PLANIFICACIÓN		**25%**
6.1 Acciones para tratar los riesgos y oportunidades		0%
6.2 Objetivos de seguridad de la información y planificación para su consecución	Se tiene claro los objetivos pero no hay una planificación total	50%

7. SOPORTE		**20%**
7.1 Recursos	No existe un presupuesto para la implementación del SGSI	0%
7.2 Competencia	No está claro el perfil para el encargados de la S.I,	30%
7.3 Concienciación	Los empleados tienen poco conocimiento sobre la existencia de políticas de seguridad	40%
7.4 Comunicación		0%
7.5 Información documentada	Faltan varios documentos que exigen el SGSI	30%
8. OPERACIÓN		**57%**
8.1 Planificación y control operacional	Existe un cronograma para el control operacional	80%
8.2 Apreciación de los riesgos de seguridad de la información	Cuenta con valoraciones de riesgos de la seguridad de la información pero no son completas.	90%
8.3 Tratamiento de los riesgos de seguridad de la información	No hay plan de tratamiento de riesgo de la seguridad de la información	0%
9. EVALUACIÓN DEL DESEMPEÑO		**17%**
9.1 Seguimiento, medición, análisis y evaluación		0%
9.2 Auditoría interna	Se ha realizado una auditoría, pero no específicamente relativas a un SGSI	50%
9.3 Revisión por la dirección		0%
10. MEJORA		**30%**
10.1 No conformidad y acciones correctivas	Se realiza algunas acciones correctivas cuando existen incidentes	60%
10.2 Mejora continua	No hay un plan de mejora continua, pero se está analizando implementar	30%
	TOTAL	**34,05%**

Análisis diferencial ISO/IEC 27002:2013

Tabla 3 Análisis Diferencial 27002:2013

CONTROL				COMENTARIOS	Evaluación	Valor	Total
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN							1
	A.5.1 Directrices de gestión de la seguridad de la información						1
		A.5.1.1	Documento de la política de seguridad de la Información	Existen algunas políticas, pero no están aprobadas por la dirección	2 - Repetible	2	
		A.5.1.2	Revisión de las políticas para la seguridad de la información	No se realiza la revisión en intervalos planificados	0 - No existente	0	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN							0,85
	A.6.1 Organización interna						1,2
		A.6.1.1	Roles y responsabilidades en seguridad de la información	No existe comité de seguridad de la información	0 - No existente	0	
		A.6.1.2	Segregación de tareas	En la asignación de tareas del auxiliar de Tics, tiene algunas tareas con respecto a la seguridad	1 - Inicial	1	
		A.6.1.3	Contacto con las autoridades	Existe comunicación con las autoridades cuando se necesita presupuesto para un determinado hardware o software	2 - Repetible	2	
		A.6.1.4	Contacto con grupos de interés especial	Se mantiene contratado un plan de soporte con respecto al firewall y antivirus	2 - Repetible	2	

		A.6.1.5	Seguridad de la información en la gestión de proyectos	cuenta un grado de seguridad en los proyectos independientemente de su naturaleza	1 - Inicial	1	
	A.6.2 Los dispositivos móviles y el teletrabajo						0,5
		A.6.2.1	Política de dispositivos móviles	cuenta políticas de uso de dispositivos móviles	1 - Inicial	1	
		A.6.2.2	Teletrabajo	La empresa no usa la modalidad de teletrabajo, cabe recalcar que en ocasiones si se realiza acceso remoto	0 - No existente	0	
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS							1,72
	A.7.1 Antes del empleo						2,5
		A.7.1.1	Investigación de antecedentes	Si se realiza comprobación de antecedentes para candidatos al puesto de trabajo	3 - Definido	3	
		A.7.1.2	Términos y condiciones del empleo	Existe un formato de confidencialidad de la información	2 - Repetible	2	
	A.7.2 Durante el empleo						0,67
		A.7.2.1	Responsabilidades de gestión	No cuenta formato de S.I para entes externos	0 - No existente	0	
		A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Las capacitaciones al personal nos son periódicas	1 - Inicial	1	

		A.7.2.3	Proceso disciplinario	El personal al momento de firmar el formato de confidencialidad de la información conoce que existe un proceso disciplinario	1 - Inicial	1	
	A.7.3 Finalización del empleo o cambio en el puesto de trabajo						2
		A.7.3.1	Responsabilidades ante la finalización o cambio	Se conoce el proceso cuando un empleado deja de laborar en la empresa	2 - Repetible	2	
A.8 GESTIÓN DE ACTIVOS							2,17
	A.8.1 Responsabilidad sobre los activos						2,5
		A.8.1.1	Inventario de activos	Se mantiene un inventario de los activos , y automatizado en los equipos de cómputo con la herramienta GLPI	2 - Repetible	2	
		A.8.1.2	Propiedad de los activos	Todos los activos tienen un custodio, se realiza un control de activos periódicamente	3 - Definido	3	
		A.8.1.3	Uso aceptable de los activos	El personal está consciente sobre el tratamiento de la información	2 - Repetible	2	
		A.8.1.4	Devolución de activos	existe control de devolución de activos	3 - Definido	3	
	A.8.2 Clasificación de la información						3
		A.8.2.1	Clasificación de la información	El personal conoce norma de las 5 S, donde la mayoría etiqueta y clasifica su información	3 - Definido	3	
		A.8.2.2	Etiquetado de la información		3 - Definido	3	
		A.8.2.3	Manipulación de los activos		3 - Definido	3	

	A.8.3 Manipulación de los soportes						1
		A.8.3.1	Gestión de soportes extraíbles	No se almacenan en entornos seguros, ni se emplean técnicas criptográficas para proteger	1 - Inicial	1	
		A.8.3.2	Eliminación de soportes	Se toma las medidas de seguridad necesarias antes de dar de baja un activo	1 - Inicial	1	
		A.8.3.3	Soportes físicos en tránsito	No cuenta un control que verifique usos indebidos o no autorizados de los activos fuera de la empresa	1 - Inicial	1	
A.9 Control de acceso							1,81
	A.9.1 Requisitos de negocio para el control de acceso						1,5
		A.9.1.1	Política de control de acceso	Existe la política pero no está aprobada	1 - Inicial	1	
		A.9.1.2	Acceso a las redes y a los servicios de red	Existen controles implementados	2 - Repetible	2	
	A.9.2 Gestión de acceso de usuario						1,33
		A.9.2.1	Registro y baja de usuarios	Existen procedimientos implementados para el registro y baja de usuarios	2 - Repetible	2	
		A.9.2.2	Provisión de acceso de usuario	No existe un procedimiento formal para asignar o renovar derechos de acceso	1 - Inicial	1	
		A.9.2.3	Gestión de privilegios de acceso	Existe gestión de privilegios restringidos	2 - Repetible	2	

		A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	No cuenta un proceso formal de gestión de información secreta	1 - Inicial	1	
		A.9.2.5	Revisión de los derechos de acceso de usuario	Se debe implantar el procedimiento formal de revisión periódica de accesos	0 - No existente	0	
		A.9.2.6	Retirada o reasignación de los derechos de acceso	Se deshabilita credenciales de acceso	2 - Repetible	2	
	A.9.3 Responsabilidades del usuario						3
		A.9.3.1	Uso de la información secreta de autenticación	La mayoría de empleados no cambia la contraseña que se otorga	1 - Inicial	3	
	A.9.4 Control de acceso a sistemas y aplicaciones						1,4
		A.9.4.1	Restricción del acceso a la información	Se realiza el control de acceso a la información, pero no se encuentra documentada	2 - Repetible	2	
		A.9.4.2	Procedimientos seguros de inicio de sesión	No cuenta un procedimiento seguro de inicio de sesión	1 - Inicial	1	
		A.9.4.3	Sistemas de gestión de contraseñas	No cuenta un sistema gestor de contraseñas	0 - No existente	0	
		A.9.4.4	Uso de utilidades con privilegios del sistema	Se controla el uso de utilidades que son capaces de invalidar los controles del sistema y de aplicación.	2 - Repetible	2	
		A.9.4.5	Control de acceso al código fuente de los programas	Se controla el acceso al código fuente de los sistemas	2 - Repetible	2	
A.10 Criptografía							
	A.10.1 Controles criptográficos						0

		A.10.1.1	Política de uso de los controles criptográficos	No existe políticas de uso de control criptográficos	0 - No existente	0	
		A.10.1.2	Gestión de claves	No cuenta política sobre uso, protección y duración de claves de cifrado	0 - No existente	0	
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO							**2,06**
	A.11.1 Áreas seguras						2,67
		A.11.1.1	Perímetro de seguridad física	Los activos críticos se encuentran protegidos dentro de un perímetro seguro	2 - Repetible	2	
		A.11.1.2	Controles físicos de entrada	El acceso a los CPD, no tienen controles de acceso , solo tiene una bitácora donde el personal registra su entrada	1 - Inicial	1	
		A.11.1.3	Seguridad de oficinas, despachos y recursos	El acceso a las oficinas e instalaciones está controlado por personal de seguridad,	1 - Inicial	1	
		A.11.1.4	Protección contra las amenazas externas y ambientales	Existen brigadas como evacuación, comunicación que tienes roles específicos con respecto a la seguridad de la información	4 - Gestionado	4	
		A.11.1.5	El trabajo en áreas seguras	Existen políticas para trabajo en áreas seguras	4 - Gestionado	4	
		A.11.1.6	Áreas de carga y descarga	Existen áreas de carga y descarga aislados de los recursos de tratamiento de la información	4 - Gestionado	4	

A.11.2 Seguridad de los equipos						1,44
	A.11.2.1	Emplazamiento y protección de equipos	Existe deficiencia en la seguridad de acceso a los CPD	1 - Inicial	1	
	A.11.2.2	Instalaciones de suministro	La mayor parte de la empresa tiene respaldo de suministro eléctrico por un lapso de hasta 4 horas	2 - Repetible	2	
	A.11.2.3	Seguridad del cableado	La red local se encuentra certificada, y el cableado eléctrico regulado	3 - Definido	3	
	A.11.2.4	Mantenimientos de los equipos	Todos los equipos de cómputo tienen su cronograma de mantenimiento anual	3 - Definido	3	
	A.11.2.5	Retirada de materiales propiedad de la empresa	Cuenta un formato para salida de equipos de la empresa, pero no siempre lo comunican	2 - Repetible	2	
	A.11.2.6	Seguridad de los equipos fuera de las instalaciones	No cuenta con documentación para el tratamiento de la información cuando un equipo sale de la empresa	0 - No existente	0	
	A.11.2.7	Reutilización o eliminación segura de equipos	Se realiza la baja de activos de información, pero no cuenta una guía de cómo realizarlo	1 - Inicial	1	
	A.11.2.8	Equipo de usuarios desatendido	No cuenta con una guía de equipos desentendidos.	0 - No existente	0	

		A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Existe la política pero no está aprobada ni comunicada al personal	1 - Inicial	1	
A.12 SEGURIDAD DE LAS OPERACIONES							1,14
	A.12.1 Procedimientos y responsabilidades operacionales						1,5
		A.12.1.1	Documentación de procedimientos de la operación	No cuenta con toda la documentación y alguna están desactualizadas	2 - Repetible	2	
		A.12.1.2	Gestión de cambios	Los cambios de versiones de código o actualización de firmware, se realizan, pero no se encuentran documentados ni justificados.	2 - Repetible	2	
		A.12.1.3	Gestión de capacidades	No cuenta un plan documentado de gestión de la capacidad para los sistema de misión critica	0 - No existente	0	
		A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	Existe entornos de pruebas y de producción	2 - Repetible	2	
	A.12.2Protección contra el software malicioso (malware)						1
		A.12.2.1	Controles contra el código malicioso	Los empleados conocen verbalmente que no deben instalar software no oficial, pero la política no está aprobada	1 - Inicial	1	
	A.12.3 Copias de Seguridad						1

	A.12.3.1	Copias de seguridad de la información	Existe unidades de almacenamiento para respaldo de la información, pero los empleados no siempre realizan un backup de los datos, con respecto a la información generada por la unidad de TICS, se respalda la información crítica	1 - Inicial	1	
A.12.4 Registros y supervisión						0.75
	A.12.4.1	Registro de eventos	No se revisa ni registra excepciones, fallos y eventos de la seguridad de la información	0 - No existente	0	
	A.12.4.2	Protección de la información de registro	No existe	0 - No existente	0	
	A.12.4.3	Registros de administración y operación	No se registra las actividades del administrador del sistema y operador del sistema	0 - No existente	0	
	A.12.4.4	Sincronización del reloj	Existe un servidor NTP	3 - Definido	3	
A.12.5 Control del software en explotación						0
	A.12.5.1	Instalación del software en explotación	No existe sistemas de control de la configuración para supervisar el software implantado	0 - No existente	0	
A.12.6 Gestión de la vulnerabilidad técnica						1

		A.12.6.1	Gestión de las vulnerabilidades técnicas	No se adoptan medidas adecuadas y oportunas en respuesta a la identificación de posibles vulnerabilidades	1 - Inicial	1	
		A.12.6.2	Restricción en la instalación de software	Existe un formato donde se establece los programas instalados, las cuentas de usuarios son limitadas	1 - Inicial	1	
	A.12.7 Consideraciones sobre la auditoría de sistemas de información						2
		A.12.7.1	Controles de auditoría de sistemas de información	Existe auditorías de los procesos de la unidad de tics, pero no específicamente de la Seguridad de la Información	2 - Repetible	2	
A.13 SEGURIDAD DE LAS COMUNICACIONES							0,88
	A.13.1 Gestión de la seguridad de redes						1
		A.13.1.1	Controles de red	El servicio de red son gestionados y controlados para proteger la información y servicios a accesos no autorizados	2 - Repetible	2	
		A.13.1.2	Seguridad de los servicios de red	No existen guías de configuración de los elementos de seguridad aprobadas por la dirección	0 - No existente	0	
		A.13.1.3	Segregación en redes	Se aplica segregación de redes	1 - Inicial	1	
	A.13.2 Intercambio de información						0,25

		A.13.2.1	Políticas y procedimientos de intercambio de información	No cuenta con políticas ni procedimientos formales para el intercambio de información	0 - No existente	0	
		A.13.2.2	Acuerdos de intercambio de información	No existe acuerdo para el intercambio de información con terceros	0 - No existente	0	
		A.13.2.3	Mensajería electrónica	No cuenta procedimientos del uso correcto de la mensajería electrónica	0 - No existente	0	
		A.13.2.4	Acuerdos de confidencialidad o no revelación	Se firma acuerdos de confidencialidad con el personal, pero no con terceros	1 - Inicial	1	
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN							1,41
	A.14.1 Requisitos de seguridad en sistemas de información						1
		A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Los requisitos relacionados con la S.I no se incluyen en los requisitos para los nuevos sistemas de información o mejoras existentes	1 - Inicial	1	
		A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No en todas los servicios públicos usan comunicaciones cifradas como HTTPS,SSL/TLS	1 - Inicial	1	
		A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Se usa comunicaciones cifradas en la consulta de facturas	1 - Inicial	1	
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte						1,22

		A.14.2.1	Política de desarrollo seguro	No cuenta políticas o no se ha comunicado al personal de TICs.	0 - No existente	0	
		A.14.2.2	Procedimiento de control de cambios en sistemas	Se usa Gitlab para llevar el control de cambios de código	2 - Repetible	2	
		A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Se verifica el funcionamiento después de un cambio pero no se hace evaluaciones de riesgo o análisis de impactos porque no cuenta un procedimiento formalmente definido.	2 - Repetible	2	
		A.14.2.4	Restricciones a los cambios en los paquetes de software	Solo los administradores pueden realizar cambios	2 - Repetible	2	
		A.14.2.5	Principios de ingeniería de sistemas seguros	No están establecidos específicamente unos principios de ingeniería segura	1 - Inicial	1	
		A.14.2.6	Entorno de desarrollo seguro	Los desarrollos se hacen en las computadoras de los empleados y luego a producción	1 - Inicial	1	
		A.14.2.7	Externalización del desarrollo de software	No se supervisa y controla el desarrollo de software externalizado	0 - No existente	0	
		A.14.2.8	Pruebas funcionales de seguridad de sistemas	No se realizan pruebas de seguridad del código	1 - Inicial	1	

		A.14.2.9	Pruebas de aceptación de sistemas	Se hacen pruebas y verificaciones para comprobar que el sistema funciona como se espera.	2 - Repetible	2	
	A.14.3 Datos de prueba						2
		A.14.3.1	Protección de los datos de prueba	Los datos utilizados son reales, no ficticios.	1 - Inicial	2	
A.15 RELACIÓN CON PROVEEDORES							1
	A.15.1 Seguridad en las relaciones con proveedores						1
		A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No cuenta con políticas relacionadas con los proveedores, lo que sí existe es un contrato cada vez que se adquiere un bien o servicio.	1 - Inicial	1	
		A.15.1.2	Requisitos de seguridad en contratos con terceros	No se firman acuerdos de confidencialidad con proveedores externos	1 - Inicial	1	
		A.15.1.3	Cadena de suministros de tecnología de la información y de las comunicaciones	En las cláusulas de contrato se hace efectiva garantía, para hacer frente a riesgos de seguridad	1 - Inicial	1	
	A.15.2 Gestión de la provisión de servicios del proveedor						1
		A.15.2.1	Control y revisión de la provisión de servicios del proveedor	No se controla la provisión de servicios del proveedor	1 - Inicial	1	
		A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Se revisan los acuerdos sólo cuando cuenta un cambio de servicio.	1 - Inicial	1	
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN							1,29

A.16.1 Gestión de incidentes de seguridad de la información y mejoras						1,29
	A.16.1.1	Responsabilidades y procedimientos	Es responsable la unidad de TICS, faltan políticas, procedimientos y no cuenta un comité de seguridad de la información	1 - Inicial	1	
	A.16.1.2	Notificación de los eventos de seguridad de la información	Las notificaciones las realizan a la unidad de Tics.	2 - Repetible	2	
	A.16.1.3	Notificación de puntos débiles de la seguridad	Las notificaciones las realizan a la unidad de Tics.	2 - Repetible	2	
	A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	La unidad de TICs evalúa los eventos de seguridad.	1 - Inicial	1	
	A.16.1.5	Respuesta a incidentes de seguridad de la información	El canal oficial de respuestas de incidentes es la unidad de TICS, no cuenta procedimientos documentados	1 - Inicial	1	
	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Cuando se soluciona un incidente grave, se comunica a toda la unidad de TICs, y se almacena la información en una bitácora.	2 - Repetible	2	
	A.16.1.7	Recopilación de evidencias	No cuenta con procedimientos para la identificación, recogida, adquisición y preservación de información que sirva como evidencia	0 - No existente	0	

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO							1,5
	A.17.1 Continuidad de la seguridad de la información						1
		A.17.1.1	Planificación de la continuidad de la seguridad de la información	No cuenta con un plan de continuidad del negocio	1 - Inicial	1	
		A.17.1.2	Implementar la continuidad de la seguridad de la información	No cuenta con un plan de continuidad del negocio	1 - Inicial	1	
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Cuenta con algunos controles pero no están documentados, y si están documentados no están aprobados	1 - Inicial	1	
	A.17.2 Redundancias						2
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Se monitorea los sistemas para mantener la disponibilidad	2 - Repetible	2	
A.18 CUMPLIMIENTO							1,53
	A.18.1 Cumplimiento de los requisitos legales y contractuales						1,4
		A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se tiene identificado la legislación aplicable para poder cumplir con los requisitos de negocio, no se mantiene negocios en otros países.	3 - Definido	3	
		A.18.1.2	Derechos de propiedad intelectual (DPI)	No cuentan con procedimientos, se usa software licenciado	1 - Inicial	1	
		A.18.1.3	Protección de los registros de la organización	Se realiza un backup de logs en físico y digital	2 - Repetible	2	

		A.18.1.4	Protección y privacidad de la información de carácter personal	La protección de la información de carácter personal la realiza cada empleado.	1 - Inicial	1	
		A.18.1.5	Regulación de los controles criptográficos	No existe regulación de controles criptográficos	0 - No existente	0	
	A.18.2 Revisiones de la seguridad de la información						1,67
		A.18.2.1	Revisión independiente de la seguridad de la información	Se realizan auditorías a los procesos de la unidad de TICs, pero no específicamente en Seguridad de la información	3 - Definido	3	
		A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Se realizan auditorías a los procesos de la unidad de TICS, pero no específicamente en Seguridad de la información	2 - Repetible	2	
		A.18.2.3	Comprobación del cumplimiento técnico	No se realizan pruebas de intrusión o evaluación de vulnerabilidades	0 - No existente	0	

5.3.1 Resultados del análisis diferencial

Con respecto a la norma ISO/IEC 27001, se observa que existe un nivel de cumplimiento total del 34.05 %, debido principalmente a que se va a implantar por primera vez un SGSI.

Con respecto a la norma ISO/IEC 27002, Se ha desglosado en un diagrama de radar (figura 4) para analizarlo, donde el radio exterior de la circunferencia representa el cumplimiento completo del nivel de seguridad de la información.

De esta forma, se pueden ver los dominios con menor cumplimiento, que son (tabla 4): Criptografía, seguridad de las comunicaciones, organización de la seguridad de la información, relación con proveedores, políticas de seguridad de la información, aspectos de seguridad de la información para la gestión de la continuidad de negocio, control de acceso.

Tabla 4. Cumplimiento de dominios ISO/IEC 27002:2013

Dominios ISO/ IEC 27002:2013	Valor
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0,85
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	1,72
A.8 GESTIÓN DE ACTIVOS	2,17
A.9 Control de acceso	1,81
A.10 Criptografía	0
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	2,06
A.12 SEGURIDAD DE LAS OPERACIONES	1,04
A.13 SEGURIDAD DE LAS COMUNICACIONES	0,63
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN	1,41
A.15 RELACIÓN CON PROVEEDORES	1
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	1,29
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	1,5
A.18 CUMPLIMIENTO	1,53

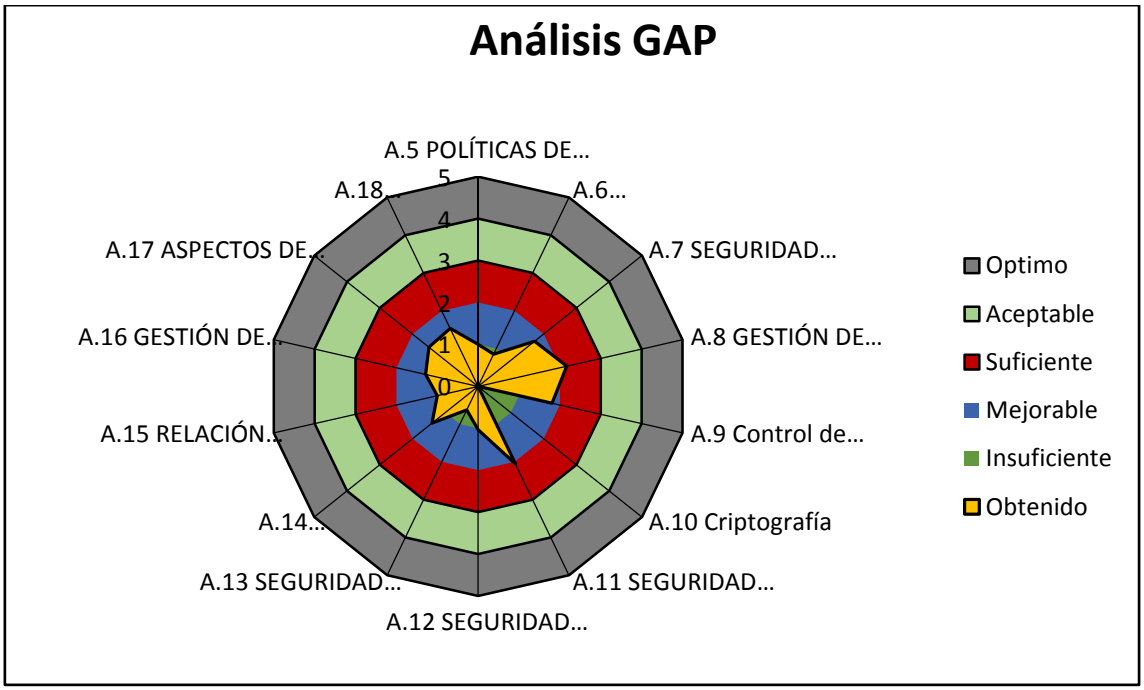


Figura 4. Análisis GAP 27002:2013

6. SISTEMA DE GESTIÓN DOCUMENTAL

Para la implantación de un correcto SGSI, el estándar ISO/IEC 27001 establece una serie de documentación obligatoria (los documentos del anexo A son obligatorio sólo si existen riesgos que impliquen su implantación). (Advisiera, S/A) para el cumplimiento normativo de la misma.

Como se menciona en la descripción de la empresa, la misma ya tiene un Sistema de Gestión de calidad ISO/IEC 9001:2015 implementado y aprobado por la alta dirección, y contiene documentación obligatoria, y políticas de alto nivel, lo que se hará es actualizar los documentos para que se pueda integrar el SGSI.

6.1 Política de la seguridad de la información

Su principal objetivo es recoger normas que deben seguir los empleados de la organización con respecto a la seguridad de la información y a la legislación vigente. Además, debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades.

Según (Advisiera, S/A), “las políticas de seguridad ISO/IEC 27001, deben cumplir con determinados requisitos que se describen a continuación.

- Debe ser redactada de una manera accesible para todo el personal de la organización.

- Debe ser aprobada por la dirección y publicitada por la misma.
- Debe estar disponible para su consulta siempre que sea necesario.
- Debe ser la referencia para la resolución de conflictos y cuestiones relativas a la seguridad de la organización.
- Debe definir responsabilidades teniendo en cuenta que éstas van asociadas a la autoridad dentro de la compañía. En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.
- Debe indicar que lo que se protege en la organización incluye tanto al personal como a la información, así como su reputación y continuidad.
- Debe ser personalizada para cada organización.
- Por último, debe señalar las normas y reglas que va a adoptar la organización y las medidas de seguridad que serán necesarias.

En lo que se refiere al contenido, la Política de Seguridad debería incluir, al menos, los siguientes cinco apartados.

Uno. Definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información.

Dos. Declaración por parte de la Dirección apoyando los objetivos y principios de la seguridad de la información.

Tres. Breve explicación de las políticas

Cuatro. Definición de responsabilidades generales y específicas, en las que se incluirán los roles pero nunca a personas concretas dentro de la organización.

Cinco. Referencias a documentación que pueda sustentar la política “.

Anexo 1. P-1 Políticas de la seguridad de la Informacion.pdf

6.2 Procedimiento de auditorías internas

Este documento describe el procedimiento de auditoría interna para el SGSI, la norma ISO/IEC 27001:2013 determina que la organización debe llevar auditorías periódicas para proporcionar información sobre el estado del SGSI que permite determinar el grado de madurez y de cumplimiento. El documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación

(una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

Anexo 2. P-2 Procedimiento auditoría interna.pdf

6.3 Gestión de indicadores

Para poder medir la eficacia de los controles de seguridad implantados es necesario el uso de distintos indicadores. El responsable de medir estos indicadores debe ser el jefe de unidad de TICs bajo la supervisión del auditor designado. Los resultados serán expuestos mensualmente. La empresa debe conservar el resultado de estas mediciones como evidencia del proceso de gestión.

Los indicadores que se van a gestionar son los siguientes:

1. Nivel de implementación del SGSI – ISO 27002
2. Incidentes de seguridad
3. Respaldos
4. Sensibilización en seguridad de la información
5. Disponibilidad de servicios informáticos
6. Equipos desprotegidos
7. Almacenamiento virtualización
8. Disponibilidad de ancho de banda
9. Controles criptográficos
10. Análisis de vulnerabilidades
11. Control de acceso

Anexo 3. P-4 Gestión de Indicadores.pdf

6.4 Procedimiento de revisión por dirección

La Dirección de la empresa es la encargada de la revisión del cumplimiento de los aspectos de seguridad relativa a la información, siendo la normativa ISO 27001 en su aparatado 9.3 la que establece que:

La revisión por la dirección debe incluir consideraciones sobre:

a. El estado de las acciones con relación a las revisiones previas por la dirección
b. Los cambios en las cuestiones externas e internas que sean pertinentes al Sistema de Gestión de Seguridad de la Información
c. La información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a:
    1. No conformidades y acciones correctivas
    2. Seguimiento y resultados de las mediciones
    3. Resultados de auditoría, y

4. El cumplimiento de los objetivos de seguridad de la información.

d) Los comentarios provenientes de las partes interesadas.
e) Los resultados de la apreciación del riego y el estado del plan de tratamiento de riesgos, y
f) Las oportunidades de mejora continua

Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio dentro del Sistema de Gestión de Seguridad de la Información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. (UNE-ISO/IEC 27001, 2014)
Anexo 4. P-5 Revisión por la dirección.pdf

6.5 Gestión de roles y responsabilidades

Para establecer los roles y responsabilidades para la seguridad de la información dentro de la organización, debe cumplir con los requisitos de la norma ISO 27001. La Dirección tendrá identificados claramente a las personas y sus tareas correspondientes dentro del SGSI
Anexo 5. P-6 Gestión de roles y responsabilidades.pdf

6.6 Metodología de análisis de riesgo

La metodología aplicada a la compañía bajo estudio es MAGERIT versión 3, cuyas siglas significan Metodología de Análisis y Gestión de los Sistemas de Información de la Administración, fue creada por el ministerio de administración pública de España. En otras palabras MAGERIT implementa el proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (administracionelectronica.gob.es, 2012).

Toda organización que ha planificado certificarse en ISO 27001, tiene que realizar un análisis de riesgo de sus activos y sistemas, determinando cuales son más críticos y que controles serán implantados para mitigar el riesgo.

El libro 1 de Magerit v3, manifiesta que, Magerit persigue los siguientes objetivos: y pasos.

Objetivos

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

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

Según (Cruz, Garre, Segovia, & Tortajada, 2018) MAGERIT tiene las siguientes fases:

6.6.1. Fase 1: Toma de datos y procesos de información.

Debe definirse el alcance que se ha de estudiar o analizar, ya que, dependiendo de éste, será más o menos costoso el proceso. A mayor alcance, mayor es el número de riesgos analizables

6.6.2. Fase 2: Establecimientos de parámetros

Consiste en el establecimiento de parámetros que se utilizarán durante todo el proceso de análisis de riesgos. Los parámetros que deben identificarse son los siguientes:

- **Valor de los activos**: Este parámetro tiene el objeto de asignar una valoración económica a todos los activos de una organización que se pretenden analizar. Los activos que han de ser analizados son aquellos que requiere la organización para llevar a cabo los procesos propios de la misma.

Tabla 5. Valoración de activos

Valoración	Rango	Valor
Muy alta	valor > 200.000 €	300.000 €
Alta	100.000€ < valor > 200.000 €	150.000 €
Media	50.000€ < valor > 100.000€	75.000 €
baja	10.000€ < valor > 50.000€	30.000 €
Muy Baja	valor < 10.000 €	10.000 €

- **Vulnerabilidad**: se entienden como una frecuencia de ocurrencia de una amenaza; es decir, la frecuencia con la que puede una organización sufrir alguna amenaza en concreto. Esta frecuencia de ocurrencia, o vulnerabilidad, también se plasma en una escala de valores (no se recomiendan más de cinco niveles) que tendrán que ser utilizados para todo el estudio.
  Vulnerabilidad = Frecuencia estimada / Días del año
  Ejemplo: Vulnerabilidad = 365/365 = 1

Tabla 6. Frecuencia de vulnerabilidades

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada 2 semanas	26/365 = 0,07123
Frecuencia media	1 vez cada 2 meses	6/365 = 0,016438
Frecuencia baja	1 vez cada 6 meses	2/365=0,005479
Frecuencia muy baja	1 vez al año	1/365=0,002739

- **Impacto:** se entiende por impacto el tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él. Para realizar este análisis a priori, también debe realizarse una estimación por rango de impactos; es decir, hay que pensar en los diferentes niveles de impacto que se quieren utilizar, y a partir de ahí asignar el porcentaje de valor que se estima que puede perderse en cada caso.

Tabla 7. Rango de impactos

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

- **Efectividad del control de seguridad:** A la hora de reducir un riesgo, hay que tener en cuenta que las medidas de seguridad tienen dos modos de actuar contra él: o bien reducen la vulnerabilidad (la frecuencia de ocurrencia), o bien reducen el impacto que provoca dicho riesgo.

Tabla 8.variación de impacto

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

6.6.3 Fase 3. Análisis de activos.

Consiste en identificar cuáles son los activos que posee la organización y que necesita para llevar a cabo sus actividades, puesto que solamente se deberían analizar aquellos activos que estén dentro de dicho alcance.

- **Activos físicos.** Serían todos los activos de tipo hardware que se utilizan en la organización: ordenadores, servidores, portátiles, PDA, teléfonos móviles, impresoras, etc.
- **Activos lógicos**. Serían todos los elementos de software que se utilizan: sistemas operativos, aplicaciones propias, paquetes cerrados de mercado, procesos bach, etc.
- **Activos de personal.** Son las personas, desde el punto de vista de roles o perfiles que intervienen en el desarrollo de las actividades de la organización: responsable de seguridad, administrador de la red, personal de administración, secretarios, usuarios, etc.
- **Activos de entorno e infraestructura**. Son todos los elementos que posee la organización y que necesita para que el resto pueda funcionar correctamente. Son, por ejemplo, los sistemas de aire acondicionado o el cableado de datos y de corriente eléctrica, etc.
- **Activos intangibles.** Son aquellos elementos que directamente no posee la organización pero que son importantes para ella, como pueden ser la imagen corporativa, la credibilidad, la confianza de los clientes, el know how, etc.

6.6.4 Fase 4: Análisis de amenazas

Son aquellas situaciones que podrían llegar a darse en una organización y que desembocarían en un problema de seguridad ejemplo:

- **Accidentes,** Son aquellas situaciones no provocadas voluntariamente y que muchas veces no pueden evitarse, sino que suceden por efectos naturales. Dentro de esta categoría de accidentes existen diferentes tipos, como: físicos (inundación, incendio, terremoto, explosión, etc.), averías, interrupciones de los servicios esenciales (cortes en el suministro eléctrico, en las telecomunicaciones, etc.) y accidentes mecánicos o electromagnéticos (choque, caída, radiación, etc.)
- **Errores,** situaciones que son cometidas de forma involuntaria, por el propio desarrollo de las actividades diarias de la organización, por desconocimiento o por descuido del personal de ésta o de terceros que son contratados por la propia organización.
- **Amenazas intencionales presenciales,** son las provocadas por el propio personal de la organización de forma voluntaria al realizar acciones que sabe que provocan un daño, tanto desde el punto de vista físico como desde el lógico. Ejemplo: Acceso físico no autorizado, acceso lógico no autorizado, indisponibilidad de recursos.
- **Amenazas intencionales remotas,** amenazas provocadas por terceras personas, es decir, por personas ajenas a nuestra organización y que consiguen dañarla.

6.6.5 Fase 5: Establecimiento de vulnerabilidades.

Se entienden aquellos agujeros que tenemos en nuestra seguridad y que permiten que una amenaza pueda dañar un activo. En MAGERIT, a pesar de que no es necesario listar las vulnerabilidades, sí que es necesario tenerlas en cuenta para poder estimar la frecuencia de ocurrencia de una determinada amenaza sobre un activo.

6.6.6 Fase 6: Establecimiento de impactos.

Se definen como las consecuencias que provoca en la organización el hecho de que una cierta amenaza, aprovechando una determinada vulnerabilidad, afecte a un activo.

6.6.7 Fase 7: Análisis de riesgo intrínseco

Se puede realizar el estudio de los riesgos actuales a los que está sometida una organización.

Riesgo = Valor del activo × Vulnerabilidad × Impacto

6.6.8 Fase 8: Influencia de Salvaguardias

Consiste en tratar de escoger la mejor solución de seguridad que me permita reducirlos (Preventivos y correctivos).

6.6.9 Fase 9: Análisis de riesgo efectivo

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

Riesgo intrínseco

Valor activo × Vulnerabilidad × Impacto

Riesgo efectivo

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

6.6.10 Fase 10: Evaluación de riesgo

Esta última fase consiste en la toma de decisiones por parte de la organización sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos

Se deberá de disminuir todos los riesgos por debajo del umbral de riesgos que es el punto en que una organización considera que los riesgos a los que se encuentra expuesta no son aceptables. Para gestionar los riesgos en una empresa pueden tomarse tres decisiones:

- Reducirlos
- Transferirlos
- Aceptarlos
- Eliminarlos

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

- **Establecer prioridades,** asignar prioridad a los riesgos que deben de reducirse en primer lugar.
- **Planteamiento del análisis de coste / beneficio,** para cada medida comprobar si el coste de la misma supera el beneficio.

- **Selección de controles definitivos,** una vez analizado el coste/beneficio de todos los controles, hay que seleccionar definitivamente los que tendrá que implantar la organización para reducir los riesgos hasta situarlos por debajo de su umbral de riesgo.
- **Asignación de responsabilidades,** asignar responsable para la implantación de los controles.
- **Implantación de controles, c**onsiste en realizar la implantación de los controles de seguridad designados, teniendo en cuenta que no forzosamente los controles que se implanten han de ser técnicos, sino que pueden ser controles organizativos o procedimentales.

6.6.11. Propietario del riesgo

Según (ISO 27000.ES, S/A), El propietario del riesgo es la persona o entidad con responsabilidad y autoridad para gestionar un riesgo. En este caso será la Unidad de TIC junto con el responsable de la seguridad de la información

6.7 Declaración de aplicabilidad (SoA)

Documento que detalla los objetivos de control aplicables al SGSI, estos objetivos se basan en el rendimiento de los medios de valoración y tratamiento de los riesgos, responsabilidades contractuales y requisitos legales o del negocio de la empresa para la seguridad de la información. (ISO Tools Excellence, 2014).

Tabla 9.Declaración de aplicabilidad

CONTROL			COMENTARIOS	Aplicabilidad
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
	A.5.1 Directrices de gestión de la seguridad de la información			
	A.5.1.1	Documento de la política de seguridad de la Información	Disponen de algunas políticas de seguridad, pero no están aprobadas por la Dirección	Aplica
	A.5.1.2	Revisión de las políticas para la seguridad de la información	La Política de Seguridad debe ser revisada y mantenerse actualizada por la Dirección. Aún no existe un registro donde aparezcan las actualizaciones acometidas sobre la misma	Aplica

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1 Organización interna				
	A.6.1.1	Roles y responsabilidades en seguridad de la información	No existe comité de seguridad de la información, La dirección tiene que comprometerse con la implementación del SGSI y velar por el cumplimiento de las políticas y normativas de seguridad.	Aplica
	A.6.1.2	Segregación de tareas	En la asignación de tareas del auxiliar de Tics, tiene algunas tareas con respecto a la seguridad.	Aplica
	A.6.1.3	Contacto con las autoridades	Requerido para norma y establecer procedimientos internos	Aplica
	A.6.1.4	Contacto con grupos de interés especial	Se mantiene contratado un plan de soporte con respecto al firewall y antivirus, pero falta otros en seguridad de la información	Aplica
	A.6.1.5	Seguridad de la información en la gestión de proyectos	Cuenta un grado de seguridad en los proyectos independientemente de su naturaleza, pero no hay documentación oficial	Aplica
A.6.2 Los dispositivos móviles y el teletrabajo				
	A.6.2.1	Política de dispositivos móviles	Cuenta con algunas políticas de uso de dispositivos móviles	Aplica
	A.6.2.2	Teletrabajo	La empresa no usa la modalidad de teletrabajo, cabe recalcar que en ocasiones si se realiza acceso remoto	Aplica
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS				
A.7.1 Antes del empleo				
	A.7.1.1	Investigación de antecedentes	Si se realiza comprobación de antecedentes para candidatos al puesto de trabajo	Aplica

A.7.1.2	Términos y condiciones del empleo	Existe un formato de confidencialidad de la información	Aplica
A.7.2 Durante el empleo			
A.7.2.1	Responsabilidades de gestión	No cuenta formato de S.I para entes externos	Aplica
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Las capacitaciones al personal nos son periódicas	Aplica
A.7.2.3	Proceso disciplinario	El personal al momento de firmar el formato de confidencialidad de la información conoce que existe un proceso disciplinario	Aplica
A.7.3 Finalización del empleo o cambio en el puesto de trabajo			
A.7.3.1	Responsabilidades ante la finalización o cambio	Se conoce el proceso cuando un empleado deja de laborar en la empresa	Aplica
A.8 GESTIÓN DE ACTIVOS			
A.8.1 Responsabilidad sobre los activos			
A.8.1.1	Inventario de activos	Se mantiene un inventario de los activos, y automatizado en los equipos de cómputo con la herramienta GLPI, se debe revisar que todos los activos que están en el alcance del SGSI estén inventariados.	Aplica
A.8.1.2	Propiedad de los activos	Todos los activos tienen un custodio, se realiza un control de activos periódicamente	Aplica
A.8.1.3	Uso aceptable de los activos	El personal está consciente sobre el tratamiento de la información, pero no existen políticas aprobadas.	Aplica
A.8.1.4	Devolución de activos	Existe control de devolución de activos	Aplica
A.8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información	El personal conoce norma de las 5 S, donde la mayoría etiqueta y clasifica su información, revisiones	Aplica
A.8.2.2	Etiquetado de la información		Aplica

A.8.2.3	Manipulación de los activos	periódicas por parte del responsable de seguridad.	Aplica
A.8.3 Manipulación de los soportes			
A.8.3.1	Gestión de soportes extraíbles	No se almacenan en entornos seguros, ni se emplean técnicas criptográficas para proteger	Aplica
A.8.3.2	Eliminación de soportes	Se toma las medidas de seguridad necesarias antes de dar de baja un activo	Aplica
A.8.3.3	Soportes físicos en tránsito	No cuenta un control que verifique usos indebidos o no autorizados de los activos fuera de la empresa	Aplica
A.9 Control de acceso			
A.9.1 Requisitos de negocio para el control de acceso			
A.9.1.1	Política de control de acceso	Existe la política pero no está aprobada	Aplica
A.9.1.2	Acceso a las redes y a los servicios de red	Existen controles implementados	Aplica
A.9.2 Gestión de acceso de usuario			
A.9.2.1	Registro y baja de usuarios	Existen procedimientos implementados para el registro y baja de usuarios	Aplica
A.9.2.2	Provisión de acceso de usuario	Procedimiento formal para asignar o renovar derechos de acceso	Aplica
A.9.2.3	Gestión de privilegios de acceso	Existe gestión de privilegios restringidos por rol de usuario	Aplica
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Proceso formal de gestión de información secreta	Aplica
A.9.2.5	Revisión de los derechos de acceso de usuario	Se debe implantar el procedimiento formal de revisión periódica de accesos	Aplica
A.9.2.6	Retirada o reasignación de los derechos de acceso	Se deshabilita credenciales de acceso	Aplica
A.9.3 Responsabilidades del usuario			

A.9.3.1	Uso de la información secreta de autenticación	La mayoría de empleados no cambia la contraseña que se otorga	Aplica
A.9.4 Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción del acceso a la información	Se realiza el control de acceso a la información, pero no se encuentra documentada	Aplica
A.9.4.2	Procedimientos seguros de inicio de sesión	Elaborar un procedimiento para inicio de sesión seguro	Aplica
A.9.4.3	Sistemas de gestión de contraseñas	Control necesario ya que no cuenta un sistema gestor de contraseñas	Aplica
A.9.4.4	Uso de utilidades con privilegios del sistema	Se controla el uso de utilidades que son capaces de invalidar los controles del sistema y de aplicación.	Aplica
A.9.4.5	Control de acceso al código fuente de los programas	El acceso solo es para la unidad de TICs	Aplica
A.10 Criptografía			
A.10.1 Controles criptográficos			
A.10.1.1	Política de uso de los controles criptográficos	Se debería tener controles criptográficos para algunos servicios de acceso	Aplica
A.10.1.2	Gestión de claves	Política sobre uso, protección y duración de claves de cifrado	Aplica
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	Mejorar el perímetro de seguridad física	Aplica
A.11.1.2	Controles físicos de entrada	Implementar controles de acceso a los CPD	Aplica
A.11.1.3	Seguridad de oficinas, despachos y recursos	Hay personal que accede a oficinas, despachos y recursos.	Aplica
A.11.1.4	Protección contra las amenazas externas y ambientales	Pueden ocurrir amenazas externas y ambientales que afecten a los activos de información de la organización.	Aplica

A.11.1.5	El trabajo en áreas seguras	Existen políticas para trabajo en áreas seguras	Aplica
A.11.1.6	Áreas de carga y descarga	Existen áreas de carga y descarga aislados de los recursos de tratamiento de la información	Aplica
A.11.2 Seguridad de los equipos			
A.11.2.1	Emplazamiento y protección de equipos	Se debe proteger y ubicar los equipos de manera segura para protegerse de los riesgos de las amenazas y los riesgos ambientales.	Aplica
A.11.2.2	Instalaciones de suministro	Asegurar el funcionamiento de los equipos a pesar de fallos en instalaciones de suministro	Aplica
A.11.2.3	Seguridad del cableado	Se debe proteger el cableado eléctrico y datos	Aplica
A.11.2.4	Mantenimientos de los equipos	Asegurar el correcto funcionamiento del equipo de cómputo	Aplica
A.11.2.5	Retirada de materiales propiedad de la empresa	Se debe autorizar la salida de equipo de cómputo	Aplica
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Proteger el tratamiento de la información cuando los equipos salen de la empresa	Aplica
A.11.2.7	Reutilización o eliminación segura de equipos	Formalizar el procedimiento de reutilización y baja de equipos de cómputo	Aplica
A.11.2.8	Equipo de usuarios desatendido	No cuenta con una guía de equipos desentendidos.	Aplica
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Comunicar al personal sobre buenas practicas	Aplica
A.12 SEGURIDAD DE LAS OPERACIONES			
A.12.1 Procedimientos y responsabilidades operacionales			
A.12.1.1	Documentación de procedimientos de la operación	Documentar procedimientos de operación	Aplica
A.12.1.2	Gestión de cambios	Controlar gestión de cambios	Aplica

A.12.1.3	Gestión de capacidades	Documentar la gestión de la capacidad para los sistema de misión critica	Aplica
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	Implementar entornos de pruebas y de producción	Aplica
A.12.2Protección contra el software malicioso (malware)			
A.12.2.1	Controles contra el código malicioso	Implementar políticas sobre uso de software no oficial	Aplica
A.12.3 Copias de Seguridad			
A.12.3.1	Copias de seguridad de la información	Realizar respaldo de la información crítica	Aplica
A.12.4 Registros y supervisión			
A.12.4.1	Registro de eventos	Se debe tener un registro de eventos para gestionar alertas.	Aplica
A.12.4.2	Protección de la información de registro	Proteger contra accesos no autorizados	Aplica
A.12.4.3	Registros de administración y operación	Documentar actividades del administrador del sistema y operador del sistema	Aplica
A.12.4.4	Sincronización del reloj	Todos los equipos deben estar sincronizados	Aplica
A.12.5 Control del software en explotación			
A.12.5.1	Instalación del software en explotación	Se debe contralar que la instalación del software sea hecha únicamente por personal autorizado del área de TI.	Aplica
A.12.6 Gestión de la vulnerabilidad técnica			
A.12.6.1	Gestión de las vulnerabilidades técnicas	Gestionar e identificar posibles vulnerabilidades	Aplica
A.12.6.2	Restricción en la instalación de software	Controlar la instalación de software en los servidores	Aplica
A.12.7 Consideraciones sobre la auditoría de sistemas de información			
A.12.7.1	Controles de auditoría de sistemas de información	Establecer un cronograma de auditorías internas	Aplica

A.13 SEGURIDAD DE LAS COMUNICACIONES				
A.13.1 Gestión de la seguridad de redes				
	A.13.1.1	Controles de red	Se debe proteger las redes de comunicación que están dentro del alcance del SGSI	Aplica
	A.13.1.2	Seguridad de los servicios de red	Proteger los servicios informáticos que están dentro del alcance del SGSI	Aplica
	A.13.1.3	Segregación en redes	Se aplica segregación de redes	Aplica
A.13.2 Intercambio de información				
	A.13.2.1	Políticas y procedimientos de intercambio de información	Implementar políticas y procedimientos formales para el intercambio de información	Aplica
	A.13.2.2	Acuerdos de intercambio de información	Formalizar acuerdos para el intercambio de información con terceros	Aplica
	A.13.2.3	Mensajería electrónica	No cuenta procedimientos del uso correcto de la mensajería electrónica	Aplica
	A.13.2.4	Acuerdos de confidencialidad o no revelación	Aprobar formatos de acuerdos de confidencialidad con el personal y con terceros	Aplica
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN				
A.14.1 Requisitos de seguridad en sistemas de información				
	A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Se adquieren o mejoran los sistemas de información que entran dentro del alcance del SGSI.	Aplica
	A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Controlar el acceso a los servicios públicos	Aplica
	A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Usar comunicaciones cifradas en la consultas hacia los servidores	Aplica
A.14.2 Seguridad en el desarrollo y en los procesos de soporte				
	A.14.2.1	Política de desarrollo seguro	Se llevan a cabo desarrollos dentro de la organización.	Aplica

	A.14.2.2	Procedimiento de control de cambios en sistemas	Se deben controlar los cambios que se hagan a las aplicaciones en producción de la organización.	Aplica
	A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Verificar el funcionamiento después de un cambio, evaluaciones de riesgo o análisis de impactos	Aplica
	A.14.2.4	Restricciones a los cambios en los paquetes de software	Se debe controlar estrictamente los cambios en los paquetes de software.	Aplica
	A.14.2.5	Principios de ingeniería de sistemas seguros	Establecer principios de ingeniería segura	Aplica
	A.14.2.6	Entorno de desarrollo seguro	Se debe establecer un adecuado entorno de desarrollo seguro para los sistemas que vayan a integrarse en la organización.	Aplica
	A.14.2.7	Externalización del desarrollo de software	No se supervisa y controla el desarrollo de software externalizado	Aplica
	A.14.2.8	Pruebas funcionales de seguridad de sistemas	La organización a veces hace uso de desarrollo de software externalizado	Aplica
	A.14.2.9	Pruebas de aceptación de sistemas	Realizar pruebas y verificaciones para comprobar que el sistema funciona como se espera.	Aplica
A.14.3 Datos de prueba				
	A.14.3.1	Protección de los datos de prueba	Proteger los datos en entornos de prueba ya sean internos o externos	Aplica
A.15 RELACIÓN CON PROVEEDORES				
A.15.1 Seguridad en las relaciones con proveedores				
	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Proteger la información de entes externos	Aplica
	A.15.1.2	Requisitos de seguridad en contratos con terceros	Acuerdos de confidencialidad con proveedores externos	Aplica

A.15.1.3	Cadena de suministros de tecnología de la información y de las comunicaciones	La organización compra productos de cómputo a proveedores	Aplica
A.15.2 Gestión de la provisión de servicios del proveedor			
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Se realiza controles esporádicamente.	Aplica
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Se revisan los acuerdos sólo cuando cuenta un cambio de servicio.	Aplica
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos	Pueden ocurrir incidentes eventos de seguridad de la información que se deben gestionar.	Aplica
A.16.1.2	Notificación de los eventos de seguridad de la información	Las notificaciones las realizan a la unidad de Tics.	Aplica
A.16.1.3	Notificación de puntos débiles de la seguridad	Las notificaciones las realizan a la unidad de Tics.	Aplica
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Gestionar los eventos de seguridad.	Aplica
A.16.1.5	Respuesta a incidentes de seguridad de la información	El canal oficial de respuestas de incidentes es la unidad de TICS, no cuenta procedimientos documentados	Aplica
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Formalizar documentos de mejora continua en SGSI	Aplica
A.16.1.7	Recopilación de evidencias	Recopilar y almacenar evidencias	Aplica

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
A.17.1 Continuidad de la seguridad de la información				
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	Planificar la continuidad del negocio	Aplica
	A.17.1.2	Implementar la continuidad de la seguridad de la información	Implementar acciones de mejora	Aplica
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Auditar controles para la continuidad del negocio	Aplica
A.17.2 Redundancias				
	A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Se monitorea los sistemas para mantener la disponibilidad	Aplica
A.18 CUMPLIMIENTO				
A.18.1 Cumplimiento de los requisitos legales y contractuales				
	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se debe identificar la legislación aplicable para evitar incumplimientos de las obligaciones legales.	Aplica
	A.18.1.2	Derechos de propiedad intelectual (DPI)	Cumplir con los derechos de Propiedad intelectual	Aplica
	A.18.1.3	Protección de los registros de la organización	Proteger registros contables, logs de las bases de datos, de auditoría, etc.	Aplica
	A.18.1.4	Protección y privacidad de la información de carácter personal	Proteger la información del personal	Aplica
	A.18.1.5	Regulación de los controles criptográficos	Realizar una correcta regulación de los controles criptográficos usados.	Aplica
A.18.2 Revisiones de la seguridad de la información				
	A.18.2.1	Revisión independiente de la seguridad de la información	Revisar periódicamente la seguridad de la información	Aplica

		A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Auditar el cumplimiento de política de seguridad de la información	Aplica
		A.18.2.3	Comprobación del cumplimiento técnico	Realizar pruebas de intrusión o evaluación de vulnerabilidades	Aplica

7. ANÁLISIS DE RIESGO

7.1. METODOLOGÍA PASO A PASO

Según (Magerit, 2012) El análisis de riesgos es desarrollado mediante una serie de tareas establecidas en el Método de Análisis de Riesgos MAR, las cuales se describen a continuación:

MAR.1 – Caracterización de los activos

- MAR.11 – Identificación de los activos
- MAR.12 – Dependencias entre activos
- MAR.13 – Valoración de los activos

MAR.2 – Caracterización de las amenazas

- MAR.21 – Identificación de las amenazas
- MAR.22 – Valoración de las amenazas

MAR.3 – Caracterización de las salvaguardas

- MAR.31 – Identificación de las salvaguardas pertinentes
- MAR.32 – Valoración de las salvaguardas

MAR.4 – Estimación del estado de riesgo

- MAR.41 – Estimación del impacto
- MAR.42 – Estimación del riesgo

Como primer paso se realizará la identificación y valoración de los activos:

7.1.1. Identificación de Activos

Se procede a agruparlos tal como indica la metodología MAGERIT, descrita en el libro 2 catálogo de elementos.

Instalaciones [INS], entornos donde se desempeñan actividades en la propia empresa.

Equipamiento Informático (Hardware) [HW], se clasificaran en cinco grupos:

- ✓ **HW.1** Hardware dentro del CPD TICS.
- ✓ **HW.2** Hardware dentro del CPD Central telefónica
- ✓ **HW.3** Hardware dentro del CPD P.E
- ✓ **HW.4** Hardware de la red externa.
- ✓ **HW.5** Hardware en la LAN para empleados

Software –Aplicaciones informáticas [SW], clasificadas en tres grupos:

- ✓ **SW.1** aplicaciones expuestas al exterior.
- ✓ **SW.2 a**plicaciones internas administradores
- ✓ **SW.3** aplicaciones internas usuarios en general.

Datos/Información [DI], información que es accedida desde el exterior como al interno de la empresa.

Redes de comunicación [COM], servicios y elementos que proveen acceso a la red de los CPD.
Servicios [SER], elementos necesarios para organizar los sistemas informáticos.
Equipamiento Auxiliar [EA], elementos complementarios necesarios para el funcionamiento del sistema.
Personal [PE], personal de la empresa que gestiona los activos e información para desarrollar los procesos diarios.
Claves criptográficas [CC], se emplea para proteger el secreto o autenticar las partes.

Las etiquetas permitirán identificar los activos y agruparlos, la siguiente Tabla 10 muestra los activos de acuerdo al alcance del SGSI:

Tabla 10.Inventario de activos

AMBITO	ACTIVO	CÓDIGO	UBICACIÓN	PROPIETARIO
Instalaciones [INS]	CPD TICS	[INS.1]	Unidad TICS	Personal de TICS
	CPD Central telefónica	[INS.2]	Central Telefónica	Personal de TICS
	CPD Planta Envasadora	[INS.3]	Planta Envasadora	Personal de TICS
Equipamiento Informático (Hardware) [HW]	Servidor de Virtualización	[HW.1.1]	Unidad TICS	Personal de TICS
	NVR	[HW.1.2]	Unidad TICS	Personal de TICS
	Servidor CAPITAL	[HW.1.3]	Unidad TICS	Personal de TICS
	Servidor SGC	[HW.1.4]	Unidad TICS	Personal de TICS

	Switch administrables TICs	[HW1.5]	Unidad TICS	Personal de TICS
	Servidor de respaldos personales	[HW1.6]	Unidad TICS	Personal de TICS
	Servidor de correo interno	[HW1.7]	Unidad TICS	Personal de TICS
	Central telefónica C.A	[HW.2.1]	Central Telefónica	Personal de TICS
	Firewall	[HW.2.2]	Central Telefónica	Personal de TICS
	Router	[HW.2.3]	Central Telefónica	Personal de TICS
	Switch Administrables CT	[HW.2.4]	Central Telefónica	Personal de TICS
	Hotspot C.T	[HW.2.5]	Central Telefónica	Personal de TICS
	Servidor de réplica de BD	[HW.3.1]	TICS P.E	Personal de TICS
	Central telefónica P.E	[HW.3.2]	TICS P.E	Personal de TICS
	Routers P.E	[HW.3.3]	TICS P.E	Personal de TICS
	Hotspot P.E	[HW.3.4]	TICS P.E	Personal de TICS
	Switch administrables P:E	[HW.3.5]	TICS P.E	Personal de TICS
	NVR P.E	[HW.3.6]	TICS P.E	Personal de TICS
	Servidor Capital P.E	[HW.3.7]	TICS P.E	Personal de TICS

	Hosting	[HW.4.1]	virtual	Personal de TICS
Software - Aplicaciones Informáticas [SW]	Página Web	[SW.1.1]	Hosting	Personal de TICS
	Sistema de Gestión de Proveedores	[SW.1.2]	Hosting	Personal de TICS
	Sistema de lecturación	[SW.1.3]	Unidad TICS	Personal de TICS
	App	[SW.1.4]	Hosting	Externalizado
	Postgres server	[SW.2.1]	Unidad TICS	Personal de TICS
	Capital Bussines	[SW.2.2]	Unidad TICS	Personal de TICS
	Softfloat	[SW.2.3]	Unidad TICS	Personal de TICS
	Softman	[SW.2.4]	Unidad TICS	Personal de TICS
	Sistema de turnos	[SW.2.5]	Unidad TICS	Personal de TICS
	Quipux	[SW.2.6]	Unidad TICS	Personal de TICS
	GLPI	[SW.2.7]	Unidad TICS	Personal de TICS
	OTRS	[SW.2.8]	Unidad TICS	Personal de TICS
	VMWARE	[SW.2.9]	Unidad TICS	Personal de TICS
	Toad Oracle	[SW.2.10]	Unidad TICS	Personal de TICS
	Kaspersky Security Center	[SW.2.11]	Unidad TICS	Personal de TICS
	Sophos	[SW.2.12]	Unidad TICS	Personal de TICS
	OpenFire	[SW.2.13]	Unidad TICS	Personal de TICS

	Páginas web Internas	[SW.2.14]	Unidad TICS	Personal de TICS
	Sistema gestión de control	[SW.2.16]	Unidad TICS	Personal de TICS
	DB visit	[SW.2.17]	Unidad TICS	Personal de TICS
	PrevenCs	[SW.2.18]	Unidad TICS	Personal de TICS
	Veeam	[SW.2.19]	Unidad TICS	Personal de TICS
	Docker	[SW.2.20]	Unidad TICS	Personal de TICS
	Pgadmin 4	[SW.2.21]	Unidad TICS	Personal de TICS
	Sistema de gestión de información	[SW.2.22]	Unidad TICS	Personal de TICS
	Portainer	[SW.2.23]	Unidad TICS	Personal de TICS
	Windows Server 2003	[SW.2.24]	Unidad TICS	Personal de TICS
	Windows Server 2000	[SW.2.25]	Unidad TICS	Personal de TICS
	Windows Server 2012	[SW.2.26]	Unidad TICS	Personal de TICS
	Linux Server Red Hat	[SW.2.27]	Unidad TICS	Personal de TICS
	Linux Server Centos	[SW.2.28]	Unidad TICS	Personal de TICS
	Linux Server Ubuntu	[SW.2.29]	Unidad TICS	Personal de TICS
	Ofimática	[SW3.1]	Unidad TICS	Personal de TICS
	Sistemas operativos Microsoft	[SW3.2]	Unidad TICS	Personal de TICS
Datos/ Información [DI]	Documentación de Quipux	[DI.1]	Empresa	Personal de TICS
	Información que se genera del Capital	[DI.2]	Empresa	Personal de TICS
	Información que se genera del Softfloat	[DI.3]	Empresa	Personal de TICS
	Información que se genera del Softman	[DI.4]	Empresa	Personal de TICS

	Información que se genera del Sistema de turnos	[DI.5]	Empresa	Personal de TICS
	Información que se genera del STC	[DI.6]	Empresa	Personal de TICS
	Información que se genera del Sistema de Lecturaciones	[DI.7]	Empresa	Personal de TICS
	Datos de la BD internas	[DI.8]	Empresa	Personal de TICS
	Datos de soportes y licencias	[DI.9]	Empresa	Personal de TICS
	Logs de servidores	[DI.10]	Empresa	Personal de TICS
	Información de SGC	[DI.11]		
	Información de PrevenCs	[DI.12]		
	Backups de servidores y usuarios	[DI.13]	Empresa	Personal de TICS
Redes de comunicación [COM]	Línea telefónica	[COM.1]	Empresa	Personal de TICS
	Servicio de VoIP	[COM.2]	Empresa	Personal de TICS
	Servicio acceso a datos	[COM.3]	Empresa	Personal de TICS
	Red inalámbrica	[COM.4]	Empresa	Personal de TICS
	Red Ethernet	[COM.5]	Empresa	Personal de TICS
	Internet	[COM.6]	Empresa	Personal de TICS
Servicios [SER]	Acceso remoto	[SER.1]	Empresa	Personal de TICS
	Correo electrónico	[SER.2]	Empresa	Personal de TICS
	Acceso Web Interno	[SER.3]	Empresa	Personal de TICS
	Acceso Web externo	[SER.4]	Empresa	Personal de TICS
	Monitorización de servidores y servicios	[SER.5]	Empresa	Personal de TICS
	Aplicaciones internas de gestión	[SER.6]	Empresa	Personal de TICS
	Servicios de soporte técnico firewall y antivirus	[SER.7]	Empresa	Personal de TICS

Equipamiento Auxiliar [EA]	Sistema de alimentación continua	[EA.1]	Empresa	Personal de TICS
	Corriente eléctrica	[EA.2]	Empresa	Personal de TICS
	Elementos de aire acondicionado	[EA.3]	Empresa	Personal de TICS
	Teléfonos móviles	[EA.4]	Empresa	Personal de TICS
	Biométrico	[EA.5]	Empresa	Personal de TICS
	Teléfonos fijos	[EA.6]	Empresa	Personal de TICS
Personal [PE]	Gerente General	[PE.1]	Empresa	Personal de TICS
	Jefes de unidad	[PE.2]	Empresa	Personal de TICS
	Personal TIC	[PE.3]	Empresa	Personal de TICS
Claves Criptográficas [CC]	Claves para el uso de la VPN para el acceso remoto	[CC.1]	Empresa	Personal de TICS
Soporte de información [Media]	DVD, CD, Blu-ray	[Media.1]	Unidad TICS	Personal de TICS
	Discos	[Media.2]	Unidad TICS	Personal de TICS

7.1.2. Dependencias entre activos

Hay que tener en cuenta que los activos dependen unos de otros, de manera jerarquizada. Un activo superior depende de otro activo inferior cuando la materialización de una amenaza sobre el activo inferior tiene consecuencias perjudiciales sobre el activo superior. Se define las dependencias entre activos de la siguiente manera:

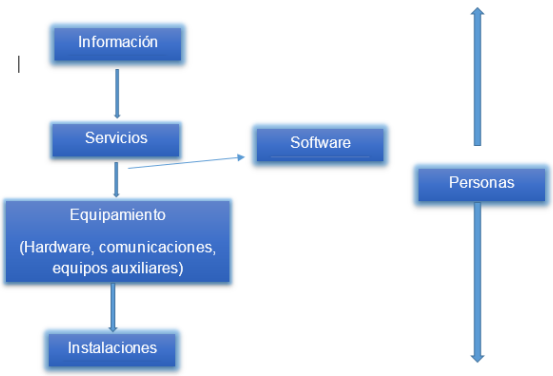


Figura 5. Dependencias de los activos

En la dependencia entre activos valorándolo cualitativamente su valor será un booleano (si o no). Ejemplo:

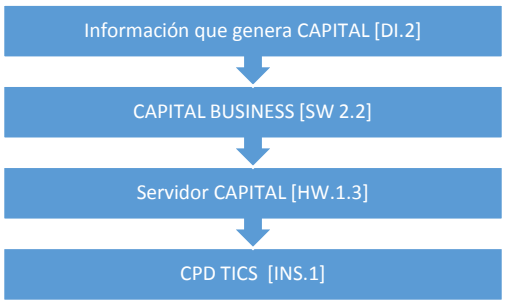


Figura 6. Ejemplo de dependencia entre activos

[DI.2] depende de [SW.2.2]
[SW2.2] depende de [HW.1.3]
[HW.1.3] depende de [INS.1]

([DI.2] → [SW.2.2]) ∧ ([SW.2.2] → [HW.1.3]) ∧ ([HW.1.3] → [INS.1])

Donde:
[DI.2] depende indirectamente de [INS.1] si y solo si existe algún activo [SW.2.2] dependa directa o indirectamente de [HW.1.3] y [HW.1.3] dependa directa o indirectamente de [INS.1]

7.1.3. Valoración de Activos

La valoración de activos se lo realiza en base a la disponibilidad, confidencialidad e integridad, esto indica el valor que tienen los activos para la empresa. A continuación se describe brevemente las diferentes dimensiones o parámetros de un activo según (administracionelectronica.gob.es, 2012).

- **Confidencialidad (C),** garantiza que la información sea accesible solamente a aquellas personas que poseen los permisos respectivos, es decir ¿Qué daño causaría que lo conociera quien no debe?
- **Integridad (I**), garantiza que los activos de información estén completos y que no exista modificaciones no autorizadas. ¿Qué perjuicio causaría que estuviera dañado o corrupto?

- **Disponibilidad (D),** garantiza que los activos sean accesibles y utilizables por los usuarios que lo requieran. ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?
- **Autenticidad (A),** propiedad o característica consiste en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad (T),** propiedad o característica consiste en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Para explicar la valoración de los activos, tomaremos como muestra a los activos [INS] Figura 7, la valoración del resto de activos se encuentran en el ANEXO 6. P-7 **Valoración de los activos.pdf**

			VALORACION DE ACTIVOS						
			VALOR		ASPECTOS CRÍTICOS				
AMBITO	ACTIVO	CÓDIGO	CUALITATIVO	CUANTITATIVO USD	D	I	C	A	T
INSTALACIONES [INS]	CDP TICS	[INS.1]	MUY ALTO	330000	9.da	10.si	10.si	10.si	4.crm
	CDP Central telefónica	[INS.2]	MUY ALTO	330000	9.da	10.si	10.si	10.si	4.crm
	CDP Planta Envasadora	[INS.3]	MUY ALTO	330000	9.da	10.si	10.si	10.si	4.crm

Figura 7. Valoración de activos [INS]

Para la valoración de activos se utiliza la combinación de una escala cuantitativa y una escala cualitativa, que se encuentra detallada en la tabla 5.

La valoración de activos con respecto a las dimensiones van desde un nivel 10, en el cual la valoración ante una pérdida de un activo por alguna amenaza es alta y crítica para la unidad de TICS, y hacia un nivel 0 que representa pérdidas despreciables o nulas para la unidad de TICS.

Según el (coordinación de contenidos, General de Modernización Administrativa, & Impulso de la Administración Electrónica, n.d.), en el apartado 4.1 muestra una escala estándar de valores y criterios en las que nos basaremos.

El activo [INS.1] tiene una valoración en cuanto a:

Disponibilidad (D) de 9.da, que significa: (Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones).

Integridad (I) de 10.si, que significa: (probablemente sea causa de un incidente excepcionalmente serio de seguridad

o dificulte la investigación de incidentes excepcionalmente serios)
Confidencialidad (C) de 10.si.
Autenticidad (A) de 10.si.
Trazabilidad (T) de 4.crm, que significa: (Dificulte la investigación o facilite la comisión de delitos).

Este nivel de valoración, se lo realizará para todos y cada uno de los activos.

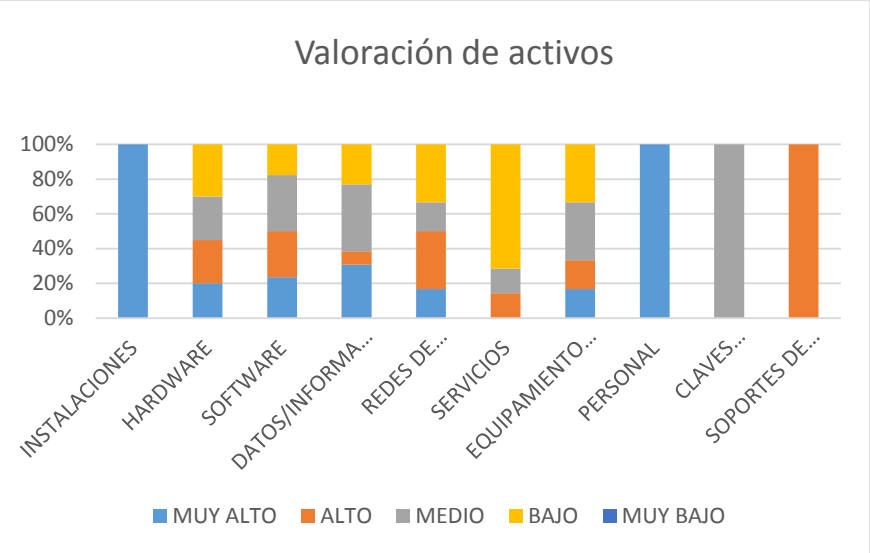


Figura 8. Resumen valoración de activos

7.1.4. Identificación de amenazas

Según (coordinación de contenidos et al., n.d.), en el apartado 5 muestra el tipo de amenazas posibles sobre los activos de un sistema de información clasificándolas en las siguientes familias.

- **Desastres naturales[N]:** ocurren sin la intervención humana
- **Amenazas de origen industrial [I]:** ocurren de forma accidental, derivados de la actividad humana.
- **Errores y fallos no intencionados [E]:** fallos no intencionales causados por las personas.
- **Ataques intencionados [A],** fallos deliberados causados por las personas.

Desastres Naturales [N]

Tabla 11. Amenazas- Desastres naturales - Fuego

[N.1]FUEGO	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media.1] [Media.2] Soportes de Información ▪ [EA] equipos auxiliar	**DIMENCIONES** 1.[D] disponibilidad
Descripción: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

Tabla 12. Amenazas- Desastres naturales - daños por agua

[N.2]DAÑOS POR AGUA	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media.1] [Media.2] Soportes de Información ▪ [EA] equipos auxiliar	**DIMENCIONES** 1.[D] disponibilidad
Descripción: Inundaciones, posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02- PERJUICIOS OCASIONADOS POR EL AGUA	

Tabla 13. Amenazas- Desastres naturales

[N.*] DESASTRES NATURALES	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar	**DIMENCIONES** 1.[D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras,... Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. Ver**: EBIOS:** 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN	

Amenazas de origen industrial [I]

Tabla 14.Amenazas- De origen industrial - Fuego

[I.1] FUEGO	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media.1] [Media.2] Soportes de Información ▪ [EA] equipos auxiliar	**DIMENCIONES** 1.[D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen**: Entorno (accidental) Humano (accidental o deliberado) **Ver**: EBIOS: 01- INCENDIO	

Tabla 15.Amenazas- De origen industrial - Daños por agua

[I.2]DAÑOS POR AGUA	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media.1] [Media.2] Soportes de Información ▪ [EA] equipos auxiliar	**DIMENCIONES** 1.[D] disponibilidad
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

Tabla 16.Amenazas- De origen industrial

[I.*] DESASTRES INDUSTRIALES	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media.1] [Media.2] Soportes de Información ▪ [EA] equipos auxiliar	**DIMENCIONES** 1.[D] disponibilidad
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 04 - SINIESTRO MAYOR	

Tabla 17.Amenazas- Desastres industriales - Contaminación mecánica

[I.3] CONTAMINACIÓN MECÁNICA	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... **Origen**: Entorno (accidental) Humano (accidental o deliberado) **Ver: EBIOS:** 03 – CONTAMINACIÓN	

Tabla 18.Amenazas- Desastres industriales - Contaminación electromagnética

[I.4] CONTAMINACIÓN ELECTROMAGNÉTICA	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 14 - EMISIONES ELECTROMAGNÉTICAS 15- RADIACIONES TÉRMICAS 16 - IMPULSOS ELECTROMAGNÉTICOS	

Tabla 19. .Amenazas- Desastres industriales - Avería de origen físico o lógico

[I.5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [SW.1] [SW.2] [SW.3] Aplicaciones ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

Tabla 20.Amenazas- Desastres industriales - Corte de suministro eléctrico

[I.6] CORTE DEL SUMINISTRO ELÉCTRICO	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

Tabla 21.Amenazas- Desastres industriales - Condiciones inadecuadas de temperatura y/o humedad

[I.7] CONDICIONES INADECUADAS DETEMPERATURA Y/O HUMEDAD	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN	

Tabla 22.Amenazas- Desastres industriales - Fallo de servicios de comunicaciones

[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	
Tipo de activos: ▪ [COM] Redes de comunicación	**DIMENCIONES** 1.[D] disponibilidad
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 13 - Pérdida de los medios de telecomunicación	

Tabla 23.Amenazas- Desastres industriales - Interrupción de otros servicios y suministros esenciales

[I.9] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	
Tipo de activos: ▪ [AUX]	**DIMENCIONES** 1.[D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: No disponible	

Tabla 24.Amenazas- Desastres industriales - Degradación de los soportes de almacenamiento de la información

[I.10] DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	
Tipo de activos: ▪ [Media.1] [Media.2] Soportes de información.	**DIMENCIONES** 1.[D] disponibilidad
Descripción: como consecuencia del paso del tiempo **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - Avería del hardware 29 - Falla de funcionamiento del hardware	

Tabla 25.Amenazas- Desastres industriales - Emanaciones electromagnéticas

[I.11] EMANACIONES ELECTROMAGNÉTICAS	
Tipo de activos: ▪ [INS] instalaciones ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media.1] [Media.2] Soportes de Información [EA] equipos auxiliar	**DIMENCIONES** 1.[C] Confidencialidad
Descripción: hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés “Transient Electromagnetic Pulse Standard”). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 17 - Interceptación de señales parásitas comprometedoras	

Errores y fallos no intencionados

Tabla 26.Amenazas- Errores y fallos no intencionados- Errores de los usuarios

[E.1] ERRORES DE LOS USUARIOS	
Tipo de activos: ▪ [CC] Claves criptógraficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [Media.1] [Media.2] Soportes de Información ▪ [SER] Servicios	**DIMENCIONES** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad

Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc**.** **Ver:** EBIOS: 38 – Error de uso

Tabla 27.Amenazas- Errores y fallos no intencionados- Errores del administrador

[E.2] ERRORES DEL ADMINISTRADOR	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [Media.1] [Media.2] Soportes de Información ▪ [SER] Servicios ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 – Error de uso	

Tabla 28.Amenazas- Errores y fallos no intencionados- Errores de monitorización(log)

[E.3] ERRORES DE MONITORIZACIÓN (log)	
Tipo de activos: ▪ [DI.10] Logs de servidores	**DIMENCIONES** 1. [I] integridad (Trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... **Ver:** EBIOS: No disponible	

Tabla 29.Amenazas- Errores y fallos no intencionados- Errores de configuración

[E.4] ERRORES DE CONFIGURACION	
Tipo de activos: ▪ [DI] Datos/información	**DIMENCIONES** 1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: No disponible	

Tabla 30.Amenazas- Errores y fallos no intencionados- deficiencias en la organización

[E.7] DEFICIENCIAS EN LA ORGANIZACIÓN	
Tipo de activos: ▪ [PE.1] [PE.2] [PE.3] personal	**DIMENCIONES** 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: No disponible	

Tabla 31.Amenazas- Errores y fallos no intencionados- Difusión de software dañino

[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones	**DIMENCIONES** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: No disponible	

Tabla 32.Amenazas- Errores y fallos no intencionados- Errores de re-encaminamiento

[E.9] ERRORES DE RE-ENCAMINAMIENTO	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [SER] Servicios ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera **Ver:** EBIOS: no disponible	

Tabla 33.Amenazas- Errores y fallos no intencionados- Errores de secuencia

[E.10] ERRORES DE SECUENCIA	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [SER] Servicios ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos. **Ver:** EBIOS: no disponible	

Tabla 34.Amenazas- Errores y fallos no intencionados- Alteración accidental de la información

[E.15] ALTERACION ACCIDENTAL DE LA INFORMACIÓN	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [Media.1] [Media.2] Soportes de Información ▪ [SER] Servicios ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [I] integridad

Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible

Tabla 35.Amenazas- Errores y fallos no intencionados- Destrucción de la información

[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [Media.1] [Media.2] Soportes de Información ▪ [SER] Servicios ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

Tabla 36.Amenazas- Errores y fallos no intencionados- Fugas de información

[E.19] FUGAS DE INFORMACIÓN	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [Media.1] [Media.2] Soportes de Información ▪ [SER] Servicios ▪ [COM] Redes de comunicación ▪ [INS.1] [INS.2] [INS.3] Instalaciones ▪ [PE] Personal	**DIMENCIONES** 1. [C] confidencialidad

Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. **Ver:** EBIOS: no disponible

Tabla 37.Amenazas- Errores y fallos no intencionados- Vulnerabilidad de los programas

[E.20] VULNERABILIDAD DE LOS PROGRAMAS	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones	**DIMENCIONES** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: No disponible	

Tabla 38.Amenazas- Errores y fallos no intencionados- Errores de mantenimiento/actualización de programas (software)

[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones	**DIMENCIONES** 1. [D] disponibilidad 2. [I] integridad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. **Ver:** EBIOS: 31 - Falla de funcionamiento del software 32 - perjuicio a la mantenibilidad del sistema de información	

Tabla 39.Amenazas- Errores y fallos no intencionados- Errores de mantenimiento/actualización de equipos(hardware)

[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE)	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. **Ver:** EBIOS: 32 - perjuicio a la mantenibilidad del sistema de información	

Tabla 40.Amenazas- Errores y fallos no intencionados- Caída del sistema por agotamiento de recursos

[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	
Tipo de activos: ▪ [SER] Servicios ▪ [COM] Redes de comunicación ▪ [HW.1] [HW.2] [HW.3] Hardware	**DIMENCIONES** 1. [D] Disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - Saturación del sistema informático	

Tabla 41.Amenazas- Errores y fallos no intencionados- Pérdida de equipos/robo

[E.25] Pérdida de equipos/Robo	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad 2.[C] confidencialidad

Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 22 - Recuperación de soportes reciclados o desechados

Tabla 42.Amenazas- Errores y fallos no intencionados- Indisponibilidad del personal

[E.28] INDISPONIBILIDAD DEL PERSONAL	
Tipo de activos: ▪ [PE] personal interno	**DIMENCIONES** 1.[D] disponibilidad
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, **Ver:** EBIOS: 42 - daño a la disponibilidad del personal	

Ataques intencionados

Tabla 43.Amenazas- Ataques intencionados- Indisponibilidad del personal

[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD(LOG)	
Tipo de activos: ▪ [DA] Datos	**DIMENCIONES** 1.[I] integridad (trazabilidad)
Descripción, **Ver:** EBIOS: no disponible	

Tabla 44.Amenazas- Ataques intencionados- Manipulación de la configuración

[A.4] MANIPULACIÓN DE LA CONFIGURACIÓN	
Tipo de activos: ▪ [DA] Datos	**DIMENCIONES** 1.[I] integridad 2.[C] confidencialidad 3.[D] disponibilidad
Descripción, prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

Tabla 45.Amenazas- Ataques intencionados- Suplantación de la identidad del usuario

[A.5] SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO	
Tipo de activos: ▪ [CC] Claves criptógraficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios	**DIMENCIONES** 1. [I] integridad 2. [C] confidencialidad 3. [A] autenticidad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. **Ver:** EBIOS: 40 - Usurpación de derecho	

Tabla 46.Amenazas- Ataques intencionados- abuso de privilegios de acceso

[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware	**DIMENCIONES** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. **Ver:** EBIOS: 39 - Abuso de derecho	

Tabla 47.Amenazas- Ataques intencionados- Uso no previsto

[A.7] USO NO PREVISTO	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media] soportes de información ▪ [INS] instalaciones ▪ [EA] Equipo auxiliar	**DIMENCIONES** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. **Ver:** EBIOS: no disponible	

Tabla 48.Amenazas- Ataques intencionados- Difusión de software dañino

[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones	**DIMENCIONES** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

Tabla 49.Amenazas- Ataques intencionados- Re-encaminamiento de mensajes

[A.9] [RE-]ENCAMINAMIENTO DE MENSAJES	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios	**DIMENCIONES** 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. **Ver:** EBIOS: no disponible	

Tabla 50.Amenazas- Ataques intencionados- Alteración de secuencia

[A.10] ALTERACIÓN DE SECUENCIA	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios	**DIMENCIONES** 1. [I] integridad
Descripción: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. **Ver:** EBIOS: 36 - Alteración de datos	

Tabla 51.Amenazas- Ataques intencionados- Acceso no autorizado

[A.11] ACCESO NO AUTORIZADO	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media] soportes de información ▪ [INS] instalaciones ▪ [EA] equipo auxiliar	**DIMENCIONES** 1. [I] integridad 2. [C] confidencialidad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. **Ver:** EBIOS: 33 - Uso ilícito del hardware	

Tabla 52.Amenazas- Ataques intencionados- Análisis de tráfico

[A.12] ANÁLISIS DE TRÁFICO	
Tipo de activos: ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”. **Ver:** EBIOS: no disponible	

Tabla 53.Amenazas- Ataques intencionados- Repudio

[A.13] REPUDIO	
Tipo de activos: ▪ [DI.10] Logs de servidores ▪ [SER] Servicios	**DIMENCIONES** 1. [I] integridad
Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro. **Ver:** EBIOS: 41 - Negación de acciones	

Tabla 54.Amenazas- Ataques intencionados- Interceptación de información (Escucha)

[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	
Tipo de activos: ▪ [COM] Redes de comunicación	**DIMENCIONES** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. **Ver:** EBIOS: 19 - escucha pasiva	

Tabla 55.Amenazas- Ataques intencionados- Modificación deliberada de la información

[A.15] MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [Media] soportes de información ▪ [INS] instalaciones	**DIMENCIONES** 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

Tabla 56.Amenazas- Ataques intencionados- Destrucción de información

[A.18] DESTRUCCIÓN DE INFORMACIÓN	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [Media] soportes de información ▪ [INS] instalaciones	**DIMENCIONES** 1. [D] Disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

Tabla 57.Amenazas- Ataques intencionados- Divulgación de información

[A.19] DIVULGACIÓN DE INFORMACIÓN	
Tipo de activos: ▪ [CC] Claves criptográficas ▪ [DI] Datos / Información ▪ [SW.1] [SW.2] [SW.3] aplicaciones ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [Media] soportes de información ▪ [INS] instalaciones	**DIMENCIONES** 1. [C] Confidencialidad
Descripción: revelación de la información **Ver:** EBIOS: 23 – Divulgación 27 – Geolocalización 34 - Copia ilegal de software	

Tabla 58.Amenazas- Ataques intencionados- Manipulación de programas

[A.22] MANIPULACIÓN DE PROGRAMAS	
Tipo de activos: ▪ [SW.1] [SW.2] [SW.3] aplicaciones	**DIMENCIONES** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 26 – Alteración de programas	

Tabla 59.Amenazas- Ataques intencionados- Manipulación de activos

[A.23] MANIPULACIÓN DE EQUIPOS	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [Media] soportes de información ▪ [EA] equipo auxiliar	**DIMENCIONES** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 25 - Sabotaje del hardware	

Tabla 60.Amenazas- Ataques intencionados- Denegación de servicio

[A.24] DENEGACIÓN DE SERVICIO	
Tipo de activos: ▪ [COM] Redes de comunicación ▪ [SER] Servicios ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware	**DIMENCIONES** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada**.** **Ver:** EBIOS: 30 – Saturación del sistema informático	

Tabla 61.Amenazas- Ataques intencionados- Robo

[A.25] Robo	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información	**DIMENCIONES** 1.[D] disponibilidad 2.[C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una	

indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 20 - Robo de soportes o documentos 21 - Robo de hardware

Tabla 62. Ataque destructivo

[A.26] ATAQUE DESTRUCTIVO	
Tipo de activos: ▪ [HW.1] [HW.2] [HW.3] [HW.4] hardware ▪ [EA] equipos auxiliar ▪ [Media.1] [Media.2] Soportes de Información ▪ [INS] instalaciones	**DIMENCIONES** 1.[D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. **Ver:** EBIOS: 05- destrucción de hardware o soportes	

Tabla 63.Amenazas- Ataques intencionados- Ocupación enemiga

[A.27] OCUPACIÓN ENEMIGA	
Tipo de activos: ▪ [INS] instalaciones	**DIMENCIONES** 1.[D] disponibilidad 2.[C] confidencialidad
Descripción: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo. **Ver:** EBIOS: no disponible	

Tabla 64.Amenazas- Ataques intencionados- Indisponibilidad del personal

[A.28] INDISPONIBILIDAD DEL PERSONAL	
Tipo de activos: ▪ [PER] Personal	**DIMENCIONES** 1.[D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, **Ver:** EBIOS: 42 - Daño a la disponibilidad del personal	

Tabla 65.Amenazas- Ataques intencionados- Extorsión

[A.29] EXTORSIÓN	
Tipo de activos: ▪ [PER] Personal	**DIMENCIONES** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. **Ver:** EBIOS: no disponible	

Tabla 66.Amenazas- Ataques intencionados- Ingeniería social

[A.30] INGENIERIA SOCIAL	
Tipo de activos: ▪ [PER] Personal	**DIMENCIONES** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. **Ver:** EBIOS: no disponible	

7.1.5. Valoración de amenazas

Una vez determinadas las amenazas que pueden perjudicar a un activo, se valora la influencia en el valor en dos sentidos:
Degradación: Cuán perjudicado resultará el [valor del] activo

Probabilidad: Cuán probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto que ocurriera.

La probabilidad de ocurrencia es compleja de determinar y de expresar, un valor cualitativo sería:

Tabla 67 . Degradación del valor

MA	Muy alta	Casi seguro	fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

La probabilidad de ocurrencia o frecuencia de ocurrencia se la valoraría de la siguiente manera:

Tabla 68. Probabilidad de ocurrencia

MA	100	Muy frecuente	A diario
A	10	Frecuente	mensualmente
M	1	Normal	Una vez al año
B	1/10(0.1)	Poco frecuente	Cada varios años
MB	1/100(0.001)	Muy poco frecuente	Siglos

Como ejemplo se muestra la amenaza [N.1], desastres naturales (Fuego) Tabla 69, para cada activo se analiza la frecuencia con la que se puede materializar la amenaza, así como su impacto en las diferentes mediciones de seguridad

Tabla 69. Valoración de amenazas [N1] Fuego

CÓDIGO	AMENAZA	ACTIVOS	FRECUENCIA	D	I	C	A	T
[N1]	FUEGO (DESASTRE NATURAL)	[INS.1]	0,1	100	0	0	0	0
		[INS.2]	0,1	100	0	0	0	0
		[INS.3]	0,1	100	0	0	0	0
		[HW.1.1]	0,1	100	0	0	0	0
		[HW.1.2]	0,1	100	0	0	0	0
		[HW.1.3]	0,1	100	0	0	0	0
		[HW.1.4]	0,1	100	0	0	0	0
		[HW1.5]	0,1	100	0	0	0	0
		[HW1.6]	0,1	100	0	0	0	0
		[HW1.7]	0,1	100	0	0	0	0
		[HW.2.1]	0,1	100	0	0	0	0
		[HW.2.2]	0,1	100	0	0	0	0
		[HW.2.3]	0,1	100	0	0	0	0
		[HW.2.4]	0,1	100	0	0	0	0
		[HW.2.5]	0,1	100	0	0	0	0
		[HW.3.1]	0,1	100	0	0	0	0
		[HW.3.2]	0,1	100	0	0	0	0
		[HW.3.3]	0,1	100	0	0	0	0
		[HW.3.4]	0,1	100	0	0	0	0
		[HW.3.5]	0,1	100	0	0	0	0
		[HW.3.6]	0,1	100	0	0	0	0
		[HW.3.7]	0,1	100	0	0	0	0
		[HW.4.1]	0,1	100	0	0	0	0
		[EA.1]	0,1	100	0	0	0	0
		[EA.2]	0,1	100	0	0	0	0
		[EA.3]	0,1	100	0	0	0	0
		[EA.4]	0,1	100	0	0	0	0
		[EA.5]	0,1	100	0	0	0	0
		[EA.6]	0,1	100	0	0	0	0
		[Media.1]	0,1	100	0	0	0	0
		[Media.2]	0,1	100	0	0	0	0

En el Anexo 7. P-8 Valoración de las amenazas.pdf, consta una tabla completa con la valoración de las amenazas para cada activo.

7.1.6. Estimación del impacto potencial

El impacto potencial es el daño causado sobre un activo en caso de materializarse una amenaza determinada. El caculo se lo realiza con la siguiente formula:

Impacto potencial = valor del activo X valor del impacto

Dónde:

Valor del activo: son los valores de cada dimensión plasmados en la valoración de los activos Figura 9; por ejemplo:

ACTIVO	CÓDIGO	CUALITATIVO	CUANTITATIVO USD	D	I	C	A	T
CDP TICS	[INS.1]	MUY ALTO	330000	9.da	10.si	10.si	10.si	4.crm

Figura 9. Valor de los activos

Para el activo [INS.1] sus valores absolutos serán (Disponibilidad 9, Integridad 10, Confidencialidad 10, Autenticidad 10 y Trazabilidad 4).

Valor del impacto: Es el valor en las dimensiones encontradas en el valor de las amenazas, Debemos aclarar que para el valor de las amenazas se tuvo en cuenta cada activo inmerso para cada tipo de amenaza. Debido a eso se tomará el valor más alto para cada activo. Como ejemplo se considera al activo [INS.1]. Figura 10.

CÓDIGO	AMENAZA	ACTIVOS	FRECUENCIA	D	I	C	A	T
[N1]	FUEGO	[INS.1]	0,1	100	0	0	0	0
[N2]	DAÑOS POR AGUA	[INS.1]	0,1	100	0	0	0	0
[N.*]	DESASTRES NATURALES	[INS.1]	0,1	100	0	0	0	0
[I.1]	FUEGO	[INS.1]	0,1	100	0	0	0	0
[I.2]	DAÑOS POR AGUA	[INS.1]	0,1	100	0	0	0	0
[I.*]	DESASTRES	[INS.1]	0,1	100	0	0	0	0
[I.11]	EMANACIONES	[INS.1]	0,1	100	0	0	0	0
[E.19]	FUGAS DE	[INS.1]	0,1	100	0	0	0	0
[A.7]	USO NO PREVISTO	[INS.1]	1	75	20	50	0	0
[A.11]	ACCESO NO	[INS.1]	0,1	0	100	100	0	0
[A.15]	MODIFICACIÓN	[INS.1]	0,1	0	100	0	0	0
[A.18]	DESTRUCCIÓN DE LA	[INS.1]	0,1	100	0	0	0	0
[A.19]	DIVULGACIÓN DE LA	[INS.1]	0,1	0	0	100	0	0
[A.26]	ATAQUE	[INS.1]	0,1	100	0	0	0	0
[A.27]	OCUPACIÓN	[INS.1]	0,1	100	0	100	0	0
			1	100	100	100	0	0

Figura 10. Valoración de amenaza para cada activo

Como resumen se muestra el cálculo del impacto potencial del activo Instalaciones Figura 11 ; el calculó completo para todos los activos está en el **Anexo 8. P-9 Impacto Potencial.pdf**

		VALOR DEL ACTIVO														
		ASPECTOS CRÍTICOS					IMPACTO(%)					IMPACTO POTENCIAL(%)				
AMBITO	ACTIVO	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
INSTALACIONES [INS]	CDP TICS	9	10	10	10	4	100	100	100	0	0	900	1000	1000	0	0
	CDP Central telefónica	9	10	10	10	4	100	100	100	0	0	900	1000	1000	0	0
	CDP Planta Envasadora	9	10	10	10	4	100	100	100	0	0	900	1000	1000	0	0

Figura 11. Cálculo de impacto potencial activo [INS]

7.1.7. Nivel de riesgo aceptable y residual

En esta fase se debe designar un límite al partir del cual se pueda decidir si asumir o no un riesgo para cada activo, aplicando controles que reduzcan los riesgos sobre los activos.

El nivel de riesgo aceptable debe ser aprobado por la dirección de la organización y se deben definir los criterios para establecer el nivel de riesgo.

El valor que la dirección asumido establecer como umbral (RIESGO ACEPTABLE) es 500, siendo este valor el que determinará la necesidad de acometer proyectos de mejora. Hasta el valor de riesgo 500 la empresa ha decidido asumir el riesgo.

Se debe aclarar que aun estableciendo controles, el riesgo se reduce, pero no se elimina, el objetivo es reducirlo por debajo del nivel de riesgo aceptable que se ha definido.

7.1.8. Cálculo del riesgo residual

Una vez obtenidos los valores del impacto potencial y utilizando la frecuencia se puede obtener el valor del riesgo, para el cálculo de riesgo se utiliza la siguiente formula:

Riesgo= impacto potencial x frecuencia

Donde:

Impacto potencial: son los valores calculados en el apartado 7.1.6 Estimación del cálculo potencial.

Frecuencia: Se usa el valor más alto del cálculo de la valoración de amenazas, por ejemplo en la figura 10, el valor de frecuencia más alta para el activo [INS.1] es **1**.

Tabla 70.Cálculo del riesgo

		FRECUENCIA	IMPACTO POTENCIAL					RIESGO				
AMBITO	**ACTIVO**	**VALOR**	**D**	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**
INSTALACIONES [INS]	CPD TICS	1	900	1000	1000	0	0	900	1000	1000	0	0
	CPD Central telefónica	1	900	1000	1000	0	0	900	1000	1000	0	0
	CPD Planta Envasadora	1	900	1000	1000	0	0	900	1000	1000	0	0
Equipamiento Informático (Hardware) [HW]	Servidor de Virtualización	1	900	500	1000	0	0	900	500	1000	0	0
	NVR	1	400	200	900	0	0	400	200	900	0	0
	Servidor CAPITAL	1	900	500	1000	0	0	900	500	1000	0	0
	Servidor SGC	1	100	400	300	0	0	100	400	300	0	0
	Switch administrables TICs	1	900	0	0	0	0	900	0	0	0	0
	Servidor de respaldos personales	1	500	500	1000	0	0	500	500	1000	0	0
	Servidor de correo interno	1	100	150	1000	0	0	100	150	1000	0	0
	Central telefónica C.A	1	100	0	0	0	0	100	0	0	0	0
	Firewall	1	900	450	900	0	0	900	450	900	0	0
	Router	1	700	450	900	0	0	700	450	900	0	0
	Switch Administrables CT	1	900	0	0	0	0	900	0	0	0	0

	Hotspot C.T	1	100	50	100	0	0	100	50	100	0	0
	Servidor de réplica de BD	1	500	450	900	0	0	500	450	900	0	0
	Central telefónica P.E	1	100	0	0	0	0	100	0	0	0	0
	Routers P.E	1	900	450	900	0	0	900	450	900	0	0
	Hotspot P.E	1	100	50	100	0	0	100	50	100	0	0
	Switch administrables P:E	1	900	0	0	0	0	900	0	0	0	0
	NVR P.E	1	400	200	900	0	0	400	200	900	0	0
	Servidor Capital P.E	1	500	500	1000	0	0	500	500	1000	0	0
	Hosting	1	500	250	1000	0	0	500	250	1000	0	0
Software - Aplicaciones Informáticas [SW]	Página Web	10	50	500	1000	1000	0	500	5000	10000	10000	0
	Sistema de Gestión de Proveedores	10	30	700	700	700	0	300	7000	7000	7000	0
	Sistema de lecturación	10	30	100	700	700	0	300	1000	7000	7000	0
	App	10	30	100	700	700	0	300	1000	7000	7000	0
	Postgres server	10	90	900	1000	1000	0	900	9000	10000	10000	0
	Capital Bussines	10	90	900	1000	1000	0	900	9000	10000	10000	0
	Softfloat	10	30	500	700	700	0	300	5000	7000	7000	0
	Softman	10	30	500	700	700	0	300	5000	7000	7000	0
	Sistema de turnos	10	90	900	1000	1000	0	900	9000	10000	10000	0
	Quipux	10	50	700	600	600	0	500	7000	6000	6000	0
	GLPI	10	30	700	700	700	0	300	7000	7000	7000	0

	OTRS	10	30	700	700	700	0	300	7000	7000	7000	0
	VMWARE	10	90	900	1000	900	0	900	9000	10000	9000	0
	Toad Oracle	10	90	900	1000	900	0	900	9000	10000	9000	0
	Kaspersky Security Center	10	90	1000	300	1000	0	900	10000	3000	10000	0
	Sophos	10	90	1000	100	1000	0	900	10000	1000	10000	0
	OpenFire	10	10	100	100	100	0	100	1000	1000	1000	0
	Páginas web Internas	10	30	100	100	100	0	300	1000	1000	1000	0
	Sistema gestión de control	10	10	100	100	100	0	100	1000	1000	1000	0
	DB visit	10	100	1000	1000	1000	0	1000	10000	10000	10000	0
	PrevenCs	10	30	100	600	700	0	300	1000	6000	7000	0
	Veeam	10	90	1000	1000	1000	0	900	10000	10000	10000	0
	Docker	10	90	1000	1000	1000	0	900	10000	10000	10000	0
	Pgadmin 4	10	90	1000	1000	1000	0	900	10000	10000	10000	0
	Sistema de gestión de información	10	90	1000	1000	1000	0	900	10000	10000	10000	0
	Portainer	10	10	100	100	100	0	100	1000	1000	1000	0
	Windows Server 2003	10	10	1000	1000	1000	0	100	10000	10000	10000	0
	Windows Server 2000	10	70	1000	1000	1000	0	700	10000	10000	10000	0
	Windows Server 2012	10	70	1000	1000	1000	0	700	10000	10000	10000	0
	Linux Server Red Hat	10	70	1000	1000	1000	0	700	10000	10000	10000	0
	Linux Server Centos	10	70	1000	1000	1000	0	700	10000	10000	10000	0
	Linux Server Ubuntu	10	70	1000	1000	1000	0	700	10000	10000	10000	0
	Ofimática	10	10	300	700	700	0	100	3000	7000	7000	0
	Sistemas operativos Microsoft	10	50	1000	1000	1000	0	500	10000	10000	10000	0

Datos/Información [DI]	Documentación de Quipux	10	500	900	900	900	100	5000	9000	9000	9000	1000
	Información que se genera del Capital	10	700	900	1000	1000	800	7000	9000	10000	10000	8000
	Información que se genera del Softfloat	10	500	800	700	700	700	5000	8000	7000	7000	7000
	Información que se genera del Softman	10	500	800	700	700	700	5000	8000	7000	7000	7000
	Información que se genera del Sistema de turnos	10	100	100	700	700	700	1000	1000	7000	7000	7000
	Información que se genera del STC	10	100	100	100	100	100	1000	1000	1000	1000	1000
	Información que se genera del Sistema de Lecturaciones	10	900	100	700	700	400	9000	1000	7000	7000	4000
	Datos de la BD internas	10	900	900	1000	1000	800	9000	9000	10000	10000	8000
	Datos de soportes y licencias	10	100	0	300	0	0	1000	0	3000	0	0
	Logs de servidores	10	800	1000	1000	1000	800	8000	10000	10000	10000	8000
	Información de SGC	10	100	100	100	100	100	1000	1000	1000	1000	1000
	Información de PrevenCs	10	300	100	900	600	600	3000	1000	9000	6000	6000

	Backups de servidores y usuarios	10	300	1000	600	1000	###	3000	10000	6000	10000	10000
Redes de comunicación [COM]	Línea telefónica	1	300	0	700	0	0	300	0	700	0	0
	Servicio de VoIP	1	300	0	0	700	0	300	0	0	700	0
	Servicio acceso a datos	1	700	700	700	700	0	700	700	700	700	0
	Red inalámbrica	1	100	700	0	0	0	100	700	0	0	0
	Red Ethernet	1	900	900	1000	1000	0	900	900	1000	1000	0
	Internet	1	300	100	1000	1000	0	300	100	1000	1000	0
Servicios [SER]	Acceso remoto	1	100	0	700	700	300	100	0	700	700	300
	Correo electrónico	1	500	700	700	700	300	500	700	700	700	300
	Acceso Web Interno	1	100	300	300	300	225	100	300	300	300	225
	Acceso Web externo	1	500	900	900	900	600	500	900	900	900	600
	Monitorización de servidores y servicios	1	100	0	0	0	0	100	0	0	0	0
	Aplicaciones internas de gestión	1	900	900	900	900	300	900	900	900	900	300
	Servicios de soporte técnico firewall y antivirus	1	700	0	1000	1000	750	700	0	1000	1000	750
Equipamiento Auxiliar [EA]	Sistema de alimentación continua	1	700	0	0	0	0	700	0	0	0	0
	Corriente eléctrica	1	900	0	0	0	0	900	0	0	0	0
	Elementos de aire acondicionado	1	300	0	0	0	0	300	0	0	0	0
	Teléfonos móviles	1	100	300	300	0	0	100	300	300	0	0
	Biométrico	1	300	300	300	0	0	300	300	300	0	0
	Teléfonos fijos	1	300	0	300	0	0	300	0	300	0	0

Personal [PE]	Gerente General	10	225	0	0	0	0	2250	0	0	0	0
	Jefes de unidad	10	225	0	0	0	0	2250	0	0	0	0
	Personal TIC	10	225	0	0	0	0	2250	0	0	0	0
Claves Criptográficas [CC]	Claves para el uso de la VPN para el acceso remoto	0,1	700	900	900	0	0	70	90	90	0	0
Soporte de información [Media]	DVD, CD, Blu-ray	1,0	300	700	900	0	0	300	700	900	0	0
	Discos	1,0	300	700	900	0	0	300	700	900	0	0

7.1.9. Riesgos críticos para el negocio

Basándose en la tabla 70. Cálculo del riesgo, se evidencia varios activos con un valor alto en riesgo, que son los que en un caso se materializara una amenaza sería perjudicial para el negocio de la organización:

Los activos con mayor nivel de riesgo son:

- Datos de la BD internas
- Logs de servidores
- Información que se genera del Capital
- Backups de servidores y usuarios
- Información que se genera del Softfloat
- Información que se genera del Softman
- Documentación de Quipux
- DB visit
- Veeam
- Docker
- Pgadmin 4
- Sistema de gestión de información
- Windows Server 2000
- Windows Server 2012
- Linux Server Red Hat
- Linux Server Centos
- Linux Server Ubuntu
- Sistemas operativos Microsoft
- Windows Server 2003
- Postgres server
- Capital Bussines
- Sistema de turnos
- VMWARE
- Toad Oracle
- Información que se genera del Sistema de Lecturaciones
- Página Web
- Información de PrevenCs
- Kaspersky Security Center
- Información que se genera del Sistema de turnos
- Sophos

7.2. Resultados

Se puede evidenciar en la Tabla 70, el valor del riesgo que tiene cada uno de los activos. Se ha dividido en dos grupos:

Primero con un valor de riesgo mayores a 1000 resaltados de color rojo, que son los que tienen prioridad urgente para mitigar el riesgo de los activos, y
Segundo con un valor de riesgo en un intervalo que va de 500 a 1000, resaltados de color amarillo que posteriormente se realizarán las gestiones para mitigar el riesgo.

Podemos observar que los activos Software-Aplicaciones Informáticas [SW] ,Datos/información[DI] y Personal [PE], son los activos más vulnerables presentando un nivel de riesgo mayor a 1000 en las dimensiones de Disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad. Estos es debido a que los datos explotados por los sistemas de información son fundamentales para la actividad de la empresa.
Un caso real sería por ejemplo la caída del Sistema CAPITAL, que es un activo fundamental para los procesos diarios de negocio.

8. PROPUESTAS DE PROYECTOS

Tras la fase de análisis de riesgo, la empresa se plantea proyectos de mejora para aumentar la seguridad de la Organización. Se priorizara según los grupos establecidos en el literal 7.6.
Los proyectos de mejora propuestos para mitigar los riesgos de los activos [SW], [D/I], [PE], son los siguientes:

- PROJ01: Plan de continuidad del Negocio
- PROJ02: Política de Backups y recuperación
- PROJ03: Plan de clasificación y tratamiento de la información
- PROJ04: Acceso seguro a la información externa/interna
- PROJ05: Formaciones continuas en temas de seguridad.

Los proyectos para el segundo grupo de activos son:

- PROJ06: Procedimiento de destrucción de soportes
- PROJ07: Implantación de políticas de la seguridad de la información
- PROJ08: Gestión de activos.
- PROJ09: Alta disponibilidad para aplicaciones que soporta la empresa.
- PROJ10: Plan de mejora de la seguridad del CPDS
- PROJ11: Gestión de incidentes de seguridad

En el Anexo 9. P-10 Propuesta de proyectos.pdf, se describe cada uno de los proyectos anteriormente descritos.

8.1. Puntos de control

Todos los proyectos tienen puntos de control, es decir deberán notificar mensualmente mediante un correo electrónico a la directiva con todas las evidencias y avances de implementación de los mismos.

8.2. Resumen de Proyectos

A continuación se muestra un resumen de esos datos:

Tabla 71. Resumen coste y temporalidad

PROYECTO	COSTE(USD)		TEMPORALIDAD	
PROJ01: Plan de continuidad del Negocio	35000	46500	1 Año	1 AÑO
PROJ02: Política de Backups y recuperación	5000		6 meses	
PROJ03: Plan de clasificación y tratamiento de la información	3000		6 meses	
PROJ04: Acceso seguro a la información externa/interna	1500		2 meses	
PROJ05: Formaciones continuas en temas de seguridad.	2000		1 Año	
PROJ06: Procedimiento de destrucción de soportes.	500	169900	1 mes	1 AÑO
PROJ07: Implantación de políticas de la seguridad de la información	14400		1 año	
PROJ08: Gestión de activos.	0		1 mes	
PROJ09: Alta disponibilidad para aplicaciones que soporta la empresa.	150000		1 año	

PROJ10: Plan de mejora de la seguridad del CPDS	5000		6 meses	
PROJ11: Gestión de incidentes de seguridad	0		2 meses	

En la tabla 70, se muestra la temporalidad que es el tiempo máximo para ejecutar los proyectos, debido a que existirán proyectos que se van a ejecutar e implementar en paralelo. En el siguiente diagrama de Gantt se muestra la planificación de ejecución de los proyectos

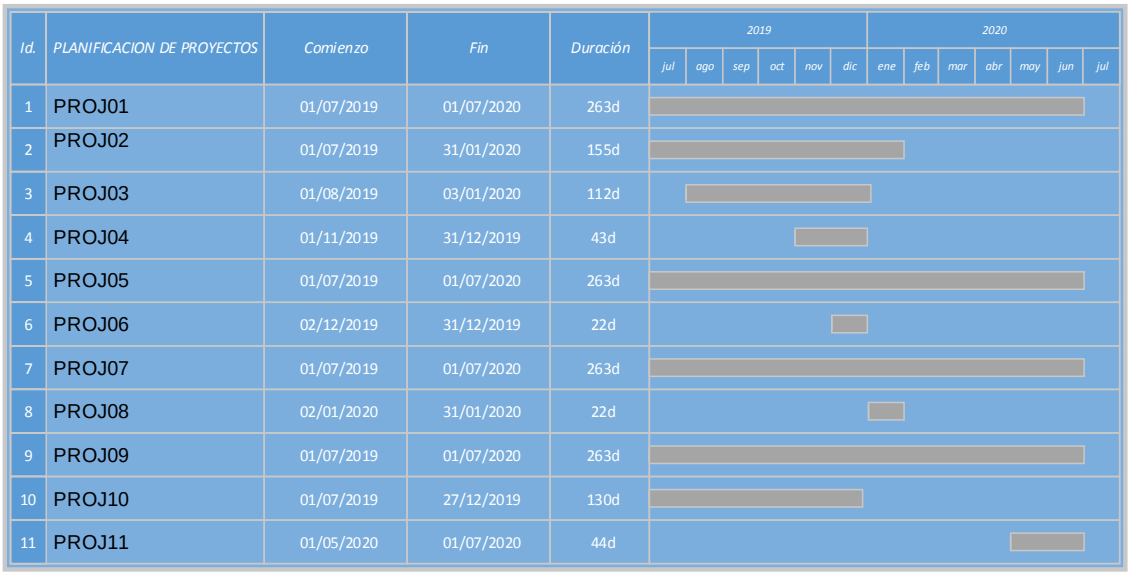


Figura 12. Diagrama de Gantt Planificación de proyectos

Todos los proyectos propuestos contribuirán a mitigar los riesgos en la organización, reduciendo la frecuencia de las amenazas y por lo tanto disminuyendo el riesgo a que están expuestos los activos.
En la Tabla 72, se observa el impacto sobre la seguridad de información que tendrán los proyectos propuestos.

Tabla 72. Cálculo de riesgo tras la ejecución de los proyectos

	FRECUENCIA	IMPACTO POTENCIAL(%)					RIESGO(%)				
ACTIVO	VALOR	D	I	C	A	T	D	I	C	A	T
CPD TICS	0,1	900	1000	1000	0	0	90	100	100	0	0
CPD Central telefónica	0,1	900	1000	1000	0	0	90	100	100	0	0
CPD Planta Envasadora	0,1	900	1000	1000	0	0	90	100	100	0	0

Servidor de Virtualización	0,1	900	500	1000	0	0	90	50	100	0	0
NVR	0,1	400	200	900	0	0	40	20	90	0	0
Servidor CAPITAL	0,1	900	500	1000	0	0	90	50	100	0	0
Servidor SGC	0,1	100	400	300	0	0	10	40	30	0	0
Switch administrables TICs	0,1	900	0	0	0	0	90	0	0	0	0
Servidor de respaldos personales	0,1	500	500	1000	0	0	50	50	100	0	0
Servidor de correo interno	0,1	100	150	1000	0	0	10	15	100	0	0
Central telefónica C.A	0,1	100	0	0	0	0	10	0	0	0	0
Firewall	0,1	900	450	900	0	0	90	45	90	0	0
Router	0,1	700	450	900	0	0	70	45	90	0	0
Switch Administrables CT	0,1	900	0	0	0	0	90	0	0	0	0
Hotspot C.T	0,1	100	50	100	0	0	10	5	10	0	0
Servidor de replica de BD	0,1	500	450	900	0	0	50	45	90	0	0
Central telefónica P.E	0,1	100	0	0	0	0	10	0	0	0	0
Routers P.E	0,1	900	450	900	0	0	90	45	90	0	0
Hotspot P.E	0,1	100	50	100	0	0	10	5	10	0	0
Switch administrables P:E	0,1	900	0	0	0	0	90	0	0	0	0
NVR P.E	0,1	400	200	900	0	0	40	20	90	0	0
Servidor Capital P.E	0,1	500	500	1000	0	0	50	50	100	0	0
Hosting	0,1	500	250	1000	0	0	50	25	100	0	0
Página Web	0,1	50	500	1000	1000	0	5	50	100	100	0
Sistema de Gestión de Proveedores	0,1	30	700	700	700	0	3	70	70	70	0
Sistema de lecturación	0,1	30	100	700	700	0	3	10	70	70	0
App	0,1	30	100	700	700	0	3	10	70	70	0
Postgres server	0,1	90	900	1000	1000	0	9	90	100	100	0
Capital Bussines	0,1	90	900	1000	1000	0	9	90	100	100	0
Softfloat	0,1	30	500	700	700	0	3	50	70	70	0

Softman	0,1	30	500	700	700	0	3	50	70	70	0
Sistema de turnos	0,1	90	900	1000	1000	0	9	90	100	100	0
Quipux	0,1	50	700	600	600	0	5	70	60	60	0
GLPI	0,1	30	700	700	700	0	3	70	70	70	0
OTRS	0,1	30	700	700	700	0	3	70	70	70	0
VMWARE	0,1	90	900	1000	900	0	9	90	100	90	0
Toad Oracle	0,1	90	900	1000	900	0	9	90	100	90	0
Kaspersky Security Center	0,1	90	1000	300	1000	0	9	100	30	100	0
Sophos	0,1	90	1000	100	1000	0	9	100	10	100	0
OpenFire	0,1	10	100	100	100	0	1	10	10	10	0
Páginas web Internas	0,1	30	100	100	100	0	3	10	10	10	0
Sistema gestión de control	0,1	10	100	100	100	0	1	10	10	10	0
DB visit	0,1	100	1000	1000	1000	0	10	100	100	100	0
PrevenCs	0,1	30	100	600	700	0	3	10	60	70	0
Veeam	0,1	90	1000	1000	1000	0	9	100	100	100	0
Docker	0,1	90	1000	1000	1000	0	9	100	100	100	0
Pgadmin 4	0,1	90	1000	1000	1000	0	9	100	100	100	0
Sistema de gestión de información	0,1	90	1000	1000	1000	0	9	100	100	100	0
Portainer	0,1	10	100	100	100	0	1	10	10	10	0
Windows Server 2003	0,1	10	1000	1000	1000	0	1	100	100	100	0
Windows Server 2000	0,1	70	1000	1000	1000	0	7	100	100	100	0
Windows Server 2012	0,1	70	1000	1000	1000	0	7	100	100	100	0
Linux Server Red Hat	0,1	70	1000	1000	1000	0	7	100	100	100	0
Linux Server Centos	0,1	70	1000	1000	1000	0	7	100	100	100	0
Linux Server Ubuntu	0,1	70	1000	1000	1000	0	7	100	100	100	0
Ofimática	0,1	10	300	700	700	0	1	30	70	70	0
Sistemas operativos Microsoft	0,1	50	1000	1000	1000	0	5	100	100	100	0
Documentación de Quipux	0,1	500	900	900	900	100	50	90	90	90	10
Información que se genera del Capital	0,1	700	900	1000	1000	800	70	90	100	100	80
Información que se genera del Softfloat	0,1	500	800	700	700	700	50	80	70	70	70
Información que se genera del Softman	0,1	500	800	700	700	700	50	80	70	70	70

Información que se genera del Sistema de turnos	0,1	100	100	700	700	700	10	10	70	70	70
Información que se genera del STC	0,1	100	100	100	100	100	10	10	10	10	10
Información que se genera del Sistema de Lecturaciones	0,1	900	100	700	700	400	90	10	70	70	40
Datos de la BD internas	0,1	900	900	1000	1000	800	90	90	100	100	80
Datos de soportes y licencias	0,1	100	0	300	0	0	10	0	30	0	0
Logs de servidores	0,1	800	1000	1000	1000	800	80	100	100	100	80
Información de SGC	0,1	100	100	100	100	100	10	10	10	10	10
Información de PrevenCs	0,1	300	100	900	600	600	30	10	90	60	60
Backups de servidores y usuarios	0,1	300	1000	600	1000	###	30	100	60	100	100
Línea telefónica	0,1	300	0	700	0	0	30	0	70	0	0
Servicio de VoIP	0,1	300	0	0	700	0	30	0	0	70	0
Servicio acceso a datos	0,1	700	700	700	700	0	70	70	70	70	0
Red inalámbrica	0,1	100	700	0	0	0	10	70	0	0	0
Red Ethernet	0,1	900	900	1000	1000	0	90	90	100	100	0
Internet	0,1	300	100	1000	1000	0	30	10	100	100	0
Acceso remoto	0,1	100	0	700	700	300	10	0	70	70	30
Correo electrónico	0,1	500	700	700	700	300	50	70	70	70	30
Acceso Web Interno	0,1	100	300	300	300	225	10	30	30	30	22,5
Acceso Web externo	0,1	500	900	900	900	600	50	90	90	90	60
Monitorización de servidores y servicios	0,1	100	0	0	0	0	10	0	0	0	0
Aplicaciones internas de gestión	0,1	900	900	900	900	300	90	90	90	90	30
Servicios de soporte técnico firewall y antivirus	0,1	700	0	1000	1000	750	70	0	100	100	75
Sistema de alimentación continua	0,1	700	0	0	0	0	70	0	0	0	0

Corriente eléctrica	0,1	900	0	0	0	0	90	0	0	0	0
Elementos de aire acondicionado	0,1	300	0	0	0	0	30	0	0	0	0
Teléfonos móviles	0,1	100	300	300	0	0	10	30	30	0	0
Biométrico	0,1	300	300	300	0	0	30	30	30	0	0
Teléfonos fijos	0,1	300	0	300	0	0	30	0	30	0	0
Gerente General	0,1	225	0	0	0	0	22,5	0	0	0	0
Jefes de unidad	0,1	225	0	0	0	0	22,5	0	0	0	0
Personal TIC	0,1	225	0	0	0	0	22,5	0	0	0	0
Claves para el uso de la VPN para el acceso remoto	0,1	700	900	900	0	0	70	90	90	0	0
DVD, CD, Blu-ray	0,1	300	700	900	0	0	30	70	90	0	0
Discos	0,1	300	700	900	0	0	30	70	90	0	0

Tras la ejecución de los proyectos, también contribuyen a mejorar el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002:2013. Ver **Anexo 10. P-11 Análisis diferencial posterior a la implementación de proyectos.pdf**

La Figura, muestra la evolución en el nivel de cumplimiento de la ISO 27002, que ha evolucionado a un nivel de madurez gestionado en algunos dominios que no alcanzaban este nivel.

Figura 13.Radar de evolución en el nivel de cumplimiento

9. AUDITORÍA DE CUMPLIMIENTO

En esta fase se lleva a cabo la evaluación de la madurez de los controles concebidos en la norma ISO/IEC 27001:2013-27002:2013, mediante una auditoría de cumplimiento, recalcando como la empresa está en una fase inicial de implementación de un SGSI, lo que se supondrá la puesta en marcha de los proyectos planteados.

9.1. Metodología

Para evaluar la auditoría de cumplimiento, se usará el Modelo de madurez de la capacidad cuyas siglas en ingles es (CMM Capability Maturity Model), que permite evaluar el nivel de cumplimiento de los requerimientos de la norma ISO/IEC 27001:20013 y un análisis de los 114 controles establecidos en la norma ISO/IEC 27002:2013 para alcanzar los diferentes objetivos de control.

La escala de valoración es la siguiente:

Tabla 73. Criterios para la evaluación del modelo de madurez

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
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante
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.

9.2. Evaluación de madurez

Para realizar la evaluación de la madurez de la seguridad, serán específicamente en los siguientes dominios:

Tabla 74. Requerimientos y dominios de control ISO/IEC 27001:2013-27002:2013

REQUERIMIENTOS 27001:2013
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora
DOMINIOS 27002:2013
A.5. Políticas de seguridad de la información
A.6. Aspectos organizativos de la seguridad de la información
A.7. Seguridad relativa a los recursos humanos.
A.8. Gestión de activos.
A.9. Control de accesos.
A.10. Criptografía.
A.11. Seguridad física y del entorno.
A.12. Seguridad en la operaciones

A.13. Seguridad de las comunicaciones.
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información.
A.15. Relaciones con proveedores
A.16. Gestión de incidentes en la seguridad de la información
A.17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
A.18. Cumplimiento.

El Anexo 11. P-12 Nivel de Cumplimiento 27001_2013.pdf se realiza una evaluación a los requerimientos de esta norma y Anexo 12. P-13 Nivel de cumplimiento 27002_2013 se realiza la evaluación de los dominios descritos en la tabla 74.

9.3. Presentación de Resultados

El resultado de la evaluación de los niveles de madurez de los requerimientos, dominios y controles implementados se los explica a continuación:

Se establece el nivel de madurez porcentual de los 7 requerimientos 27001:2013, Tabla 75, Figura 14, así:

Tabla 75. Nivel de madurez de requerimientos 27001:2013

Nivel de Madurez	requerimientos por nivel
L0	0
L1	0
L2	0
L3	0
L4	7
L5	0
TOTAL	7

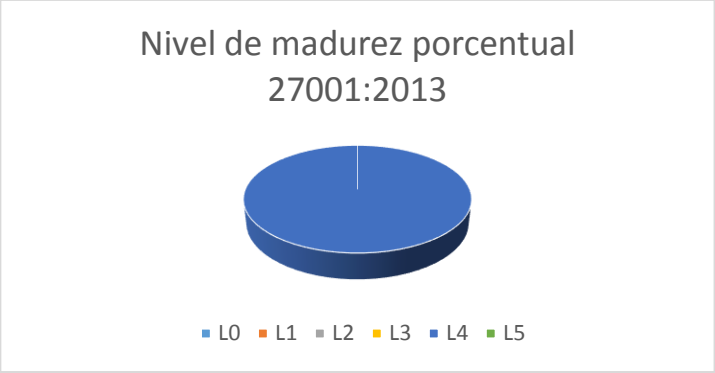


Figura 14. Nivel de madurez porcentual 27001:2013

En el siguiente diagrama de radar Figura 15 , se evidencia el nivel de cumplimiento actual vs inicial de la norma 27001:2013:

Figura 15. Diagrama de radar cumplimiento 27001:2013 actual vs inicial

Se establece el nivel de madurez porcentual de los 114 controles 27002:2013, Figura 16, así:

Tabla 76. Nivel de madurez por control

Nivel de Madurez	Controles por nivel
L0	0
L1	7
L2	7
L3	17
L4	83
L5	0
TOTAL	114

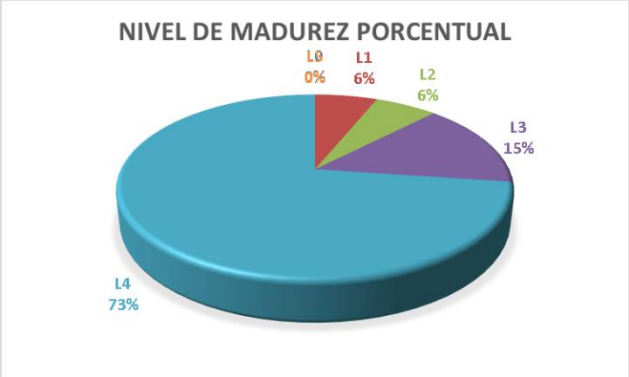


Figura 16. Nivel de madurez porcentual 27002:2013

En el siguiente diagrama de radar Figura 17 , se evidencia el nivel de cumplimiento para cada uno de los dominios de la norma 27002:2013:

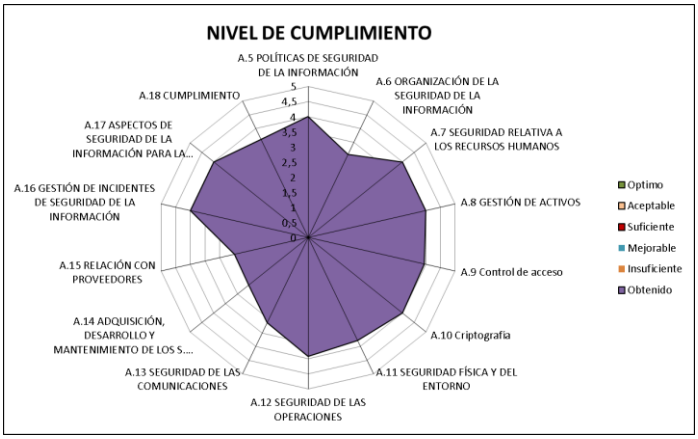


Figura 17. Nivel de cumplimiento por dominio ISO 27002:2013

Para la organización el nivel de meta objetivo es el L5- Optimizado (100%), siguiendo una mejora continua para llegar a este objetivo Figura 18:

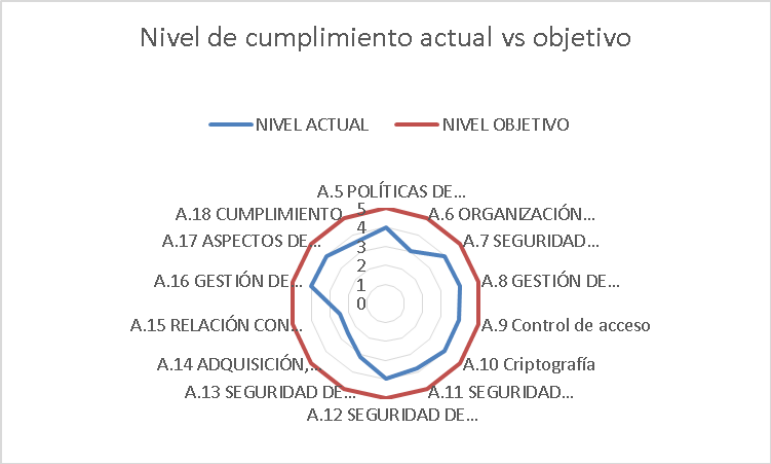
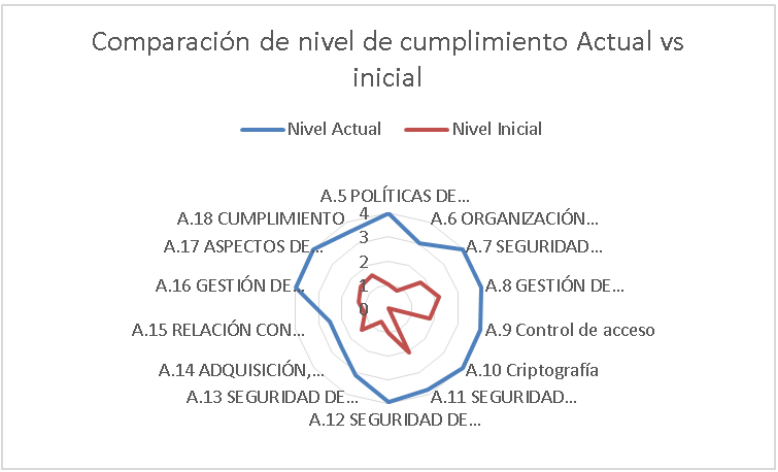


Figura 18. Nivel de cumplimiento actual vs objetivo

A demás se realiza una comparación entre el nivel de medición actual vs el nivel inicial, es después de la implementación de proyectos y políticas de seguridad. Figura 19

Figura 19. Comparación de nivel de cumplimiento Actual vs Inicial



De la evaluación de los requerimientos ISO/IEC27001:2013 se evidencia que 1 de ellos necesita atención inmediata, debido a su criticidad y 2 acciones de mejora.

Tabla 77. Resumen de no conformidades 27001

REQUERIMIENTOS 27001:2013	ACCIÓN DE MEJORA, NO CONFORMIDAD MENOR/MAYOR
4. Contexto de la Organización	2 Acciones de mejora
5. Liderazgo	1 No conformidad Mayor
6. Planificación	
7. Soporte	
8. Operación	
9. Evaluación del desempeño	
10. Mejora	

De la evaluación de los 114 controles se evidencia que 3 de ellos se necesita atención inmediata, debido a la criticidad de ellas, encontrando 3 no conformidades mayores y 1 acción de mejora.

Tabla 78. Resumen de no conformidades 27002

DOMINIOS	ACCIÓN DE MEJORA, NO CONFORMIDAD MENOR/MAYOR
5. Políticas de seguridad de la información	
6. Aspectos organizativos de la seguridad de la información	1 No conformidad Mayor
7. Seguridad relativa a los recursos humanos.	
8. Gestión de activos.	1 Acción de mejora
9. Control de accesos.	
10. Criptografía.	
11. Seguridad física y del entorno.	1 No conformidad Mayor
12. Seguridad en la operaciones	

13. Seguridad de las comunicaciones.	1 No conformidad Mayor
14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	
15. Relaciones con proveedores	
16. Gestión de incidentes en la seguridad de la información	
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	
18. Cumplimiento.	

Los detalles de las no conformidades se encuentran establecidos en el **Anexo 13. Informe de Auditoría.pdf**

10. RESULTADOS FINALES

En esta fase tiene como objetivo recopilar información y dar un formato de presentación. Esta información incluirá como mínimo los siguientes aspectos:

- Resumen Ejecutivo
- Memoria del Trabajo Final de Máster(presente documento)
- Presentación Global del PDSI
- Presentación a la Dirección
- Video de presentación del trabajo Final de Máster

11. CONCLUCIONES

- Partimos con un estado inicial de la empresa en el que la mayoría de requerimientos de la ISO/IEC 27001 y controles de la ISO/IEC 27002 estaban en un nivel inexistente e inicial. La implantación del presente SGSI dota a la empresa de las medidas de seguridad necesarias para gestionar y mitigar las amenazas detectadas en el presente proyecto, permitiendo una reducción considerable de los riesgos que están expuestos los activos.
- Se levantó un inventario y valoración de activos que permitieron realizar una evaluación y valoración de las posibles amenazas que podrían materializarse en los activos, con esta información permitió realizar el cálculo del impacto en las diferentes dimensiones de seguridad y nivel de riesgo que tienen cada uno de los activos de la empresa.
- Se analizaron los resultados anteriores permitiendo el planteamiento de varias Propuestas de Proyectos que tienen como objetivo mejorar

la seguridad de la información incluyendo coste estimado de implementación, tiempo de ejecución y puntos de control.

- Se realiza una evaluación de la madurez de los requerimientos y controles establecidos en la ISO/IEC 27001 -27002, mediante una auditoría de cumplimiento. Dando como resultado “no conformidades” que deben ser resueltas en plazos establecidos.
- Tras la realización de todas las fases mencionadas anteriormente se ha logrado mejorar el estado inicial de la seguridad de la información a demás se ha logrado la concienciación y colaboración de los empleados en materia de la seguridad de la información.
- Finalmente existe un compromiso por parte de la alta dirección de revisar y monitorear el SGSI, permitiendo retroalimentar el ciclo el Demming, asegurando que los controles o salvaguardas sigan siendo efectivas y no se produzcan desviaciones, nuevas amenazas o cambios en el contexto o en los objetivos de la empresa.

12. BIBLIOGRAFIA

administracionelectronica.gob.es. (s/d de 10 de 2012). *PAE Portal de administración electrónica.* Obtenido de administracionelectronica.gob.es: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XIKWHiJKiM8

Advisiera. (S/D de S/M de S/A). *Advisiera*. Obtenido de RGPD UE: ¿Qué es y cómo funciona?: https://advisera.com/eugdpracademy/es/que-es-la-rgpd-ue/

Cruz, D., Garre, S., Segovia, A., & Tortajada, A. (2018). *Sistema de gestión de la seguridad de la información.* Barcelona: Oberta UOC Publishing, SL.

Escuela Europea de Excelencia. (11 de 10 de 2016). *Nueva iso 9001-2015*. Obtenido de ¿Cómo integrar las normas ISO 9001 e ISO 27001?: https://www.nueva-iso-9001-2015.com/2016/10/integrar-normas-iso-9001-e-iso-27001/

Incibe. (S/D de S/M de S/A). *INCIBE.* Obtenido de Implantación de un SGSI en la empresa : https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27000.ES. (S/D de S/M de S/A). *ISO 27000.ES*. Obtenido de Glosario: http://www.iso27000.es/glosario.html

ISO Tools Excellence. (31 de 03 de 2014). *Blog especializado en Sistemas de Gestión*. Obtenido de ISO 27001 La declaración de aplicabilidad: https://www.pmg-ssi.com/2014/03/iso-27001-la-declaracion-de-aplicabilidad/

Policia Nacional del Ecuador. (27 de 12 de 2017). *Policia Nacional del Ecuador*. Obtenido de Delitos informáticos establecidos en el COIP y como prevenirlos: http://www.policiaecuador.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

UNE-ISO/IEC 27001. (10 de 2014).

Coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (n.d.). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos*. Retrieved from http://administracionelectronica.gob.es/

Magerit. (2012). *Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas*. Retrieved from http://administracionelectronica.gob.es/

13. ANEXOS