Máster universitario en Seguridad de las TIC (MISTIC)

Trabajo Final de Máster

Elaboración de un Plan Director de Seguridad para la empresa TrendTip

TrendTip

Autor: Beatriz Cantalejo García

Director: Antonio José Segovia Henares

Centro: Universitat Oberta de Catalunya

Fecha de entrega: 5 de junio de 2019

Resumen

El trabajo a desarrollar se centra en la elaboración de un plan director de seguridad de la información de un empresa online de moda cuyo objetivo es servir de escaparate a los pequeños comercios textiles y de calzado, haciendo de intermediario entre éstos y sus potenciales compradores.

El Plan Director de Seguridad de la Información está alineado con los estándares ISO 27001 e ISO 27002 y se desarrolla en seis fases:

Fase 1: La primera fase consiste en una aproximación a la situación actual de la seguridad de la información de la página online de moda a través del análisis diferencial contra las normas ISO/IEC 27001 e ISO/IEC 27002.

Fase 2: La segunda fase consiste en el desarrollo del sistema de gestión documental. Durante este proceso se elaborarán los documentos descritos en la norma ISO 27001 como obligatorios.

Fase 3: La tercera fase consiste en la realización del análisis de riesgos. Para ello, se determinarán los activos presentes en la organización y se evaluará el impacto que tiene para ella la materialización de las amenazas. La función de este análisis es determinar el nivel de riesgo al que está expuesta dicha organización y su plan de tratamiento de estos riesgos.

Fase 4: Durante esta fase se propondrán y desarrollarán aquellos proyectos que ayuden a la organización a reducir el riesgo que supone la materialización de las amenazas. Además, contribuirán a la evolución del cumplimiento ISO hasta un nivel adecuado.

Fase 5: A lo largo de esta fase se evaluará el cumplimiento de la empresa de las controles descritos en la ISO27002.

Abstract

The work to be developed focuses on the elaboration of an information security master plan for an online fashion company whose objective is to serve as a showcase for small textile and footwear businesses, acting as an intermediary between them and their potential buyers.

The Information Security Master Plan is aligned with the ISO 27001 and ISO 27002 standards and is developed in six phases:

Phase 1: The first phase consists of an approximation to the current situation of the information security of the online fashion page through differential analysis against ISO/IEC 27001 and ISO/IEC 27002.

Phase 2: The second phase consists of the development of the document management system. During this process the documents described in ISO 27001 as mandatory will be elaborated.

Phase 3: The third phase consists of carrying out the risk analysis. To this end, the assets present in the organization will be determined and the impact of the materialization of the threats on the organization will be assessed. The function of this analysis is to determine the level of risk to which the organization is exposed and its plan for dealing with these risks.

Phase 4: During this phase, projects will be proposed and developed that help the organization to reduce the risk posed by the materialization of threats. In addition, they will contribute to the evolution of ISO compliance to an appropriate level.

Phase 5: Throughout this phase, the company's compliance with the controls described in ISO27002 will be evaluated.

Contenido

Índice de tablas

Índice de figuras

1. Introducción

La forma en la que se almacenan los datos y se gestionan los procesos ha variado de forma vertiginosa a lo largo de los años. Hasta hace poco, las empresas guardaban y almacenaban sus datos en carpetas y archivadores que guardaban bajo llave, por lo que el acceso a ellas estaba limitado; mientras que la gestión de los procesos era una tarea manual y muy costosa.

En los últimos años, la incorporación e implantación de las Tecnologías de Información y comunicación (TIC) en los sistemas de información, ha transformado el modo de actuar. Este hecho ha permitido la optimización en el almacenamiento de la información (discos duros, portátiles o USB...) y la automatización de los procesos de la organización, que son soportados y gestionados en gran medida por sistemas informáticos.

En la actualidad la mayor parte de la información vital de las organizaciones se encuentra almacenada en equipos informáticos. Esto provoca que estos se encuentren expuestos a multitud de riesgos y están sujetos a sufrir diversos tipos de incidentes. Dichos riesgos pueden ser aprovechados de forma ilícita por diferentes personas comprometiendo la disponibilidad (la información debe estar lista para acceder cuando se necesite), la integridad (la información debe ser completa y correcta en cualquier momento) y/o la confidencialidad (la información solo debe ser accesible por personas autorizadas) de la información que contienen.

Es por ello, que en el actual entorno competitivo de la sociedad de la información, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas.

El presente documento contiene un plan de implementación de una plan director de seguridad para la empresa **TrendTip** basado en las normas de referencia ISO 27001 e ISO 27002. Para realizarlo se va a estructurar en 6 fases que se detallan a continuación:

Situación actual:

- Contextualización, Objetivos y Análisis Diferencial
- Sistema de Gestión Documental.
- Análisis de Riesgos
- Propuestas de Proyectos
- Auditoría de Cumplimiento
- Presentación de Resultados y Entrega de Informes

1.1 Objetivos y desafío

El aumento de los riesgos a los que están expuestos los sistemas informáticos y la necesidad de las organizaciones de preservar la confidencialidad, la integridad y la disponibilidad de sus datos han llevado a la necesidad de crear un Sistema de Gestión de la Seguridad (SGSI).

Este sistema no sólo tiene la misión de preservar y defender sus activos, también ayuda a la empresa a generar mayor confianza en sus clientes y potenciales inversores.

A día de hoy, y a pesar de que existe una normativa para la aplicación de medidas en lo relativo a la seguridad de la información, siguen apareciendo casos de robos de datos de clientes en multitudes de empresas y personas privadas.

Es de suponer que la extensa y compleja normativa genera un problema a la hora de implantar un SGSI. Pero no sólo la normativa es un problema, el factor económico tiene también un peso importante. El problema reviste en que la implantación del sistema no genera ingresos económicos para la empresa, únicamente evita que se pierda o se adultere la información y reduce el impacto si llegara a producirse. Es por ello que el beneficio que puede ocasionar su implantación no se considere suficiente en relación a su coste.

Debido a la importancia que tiene la implantación de este sistema, cada día son más las empresas concienciadas con este tema. El número de empresas y organizaciones con este sistema implantado ha aumentado de forma notoria en estos últimos años [ver Tabla 1].

Tabla 1: Evolución número de certificados ISO 27001 en 2017

Estándar	Número certificados 2016	Número certificados 2017	Evolución	Evolución
ISO 27001	33290	39501	6211	19 %

Uno de los factores que se tienen para evaluar el número de organizaciones que cuentan con un Sistema de Seguridad implantado es medir el número de certificaciones. Las certificaciones tienen como objetivo la acreditación y legitimación del producto o sistema, en este caso, el Sistema de Gestión de Seguridad de la Información.

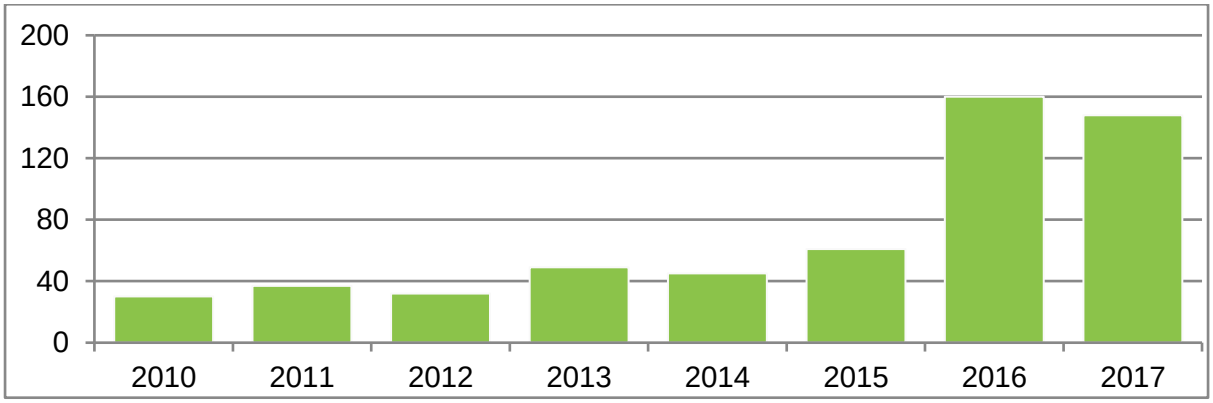


Figura 1: Evolución número de certificaciones ISO 27001. Fuente: ISO Survey 2017

En España se cuenta con un total de 803 certificaciones de Sistemas de Gestión de Seguridad en 2014, según la encuesta realizada por la ISO a finales del 2014 [ver Figura 2]. Esta cifra está muy por debajo de la de países como Japón (9161 certificaciones, más de 10 veces más).

Los objetivos que se plantean en este trabajo son:

- Establecer la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla.
- Alinear los objetivos de seguridad de la información con los requisitos del negocio
- Establecer unas guías para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información en la entidad.

1.2 Estructura del documento

El documento cuenta con un total de seis capítulos y dos anexos.

En el Capítulo 2 se da una visión general de lo que es la Seguridad explicando los tres principios que la definen: confidencialidad, integridad y disponibilidad de los datos. Se explica además el ciclo PDCA (Plan Do Check Act) en el que está basada está guía.

En el Capítulo 3 se da una visión general de empresa en estudio, los objetivos que tiene la implantación del plan director de seguridad, el alcance y un análisis diferencial donde se muestra el estado de seguridad con el que parte la organización.

En el Capítulo 4 se desarrollará el Sistema de gestión documental de la organización.

El Capítulo 5 se realiza un análisis de riesgos de la empresa propuesta. Para ello, se determinarán los activos presentes en la organización y se evaluará el impacto que tiene para ella la materialización de las amenazas. La función de este análisis es determinar el nivel de riesgo al que está expuesta dicha organización y su plan de tratamiento de estos riesgos

El Capítulo 6 consta de los proyectos propuestos por la organización que ayudan a la a reducir el riesgo que supone la materialización de las amenazas evaluadas en el análisis de riesgos. Además, contribuirán a la evolución del cumplimiento ISO hasta un nivel adecuado.

En el Capítulo 7 se realiza una evaluación de cumplimiento de la organización una vez realizados el análisis de riesgos y la implantación de los proyectos propuestos.

En el Capítulo 8 se establecen las conclusiones sacadas del trabajo, mostrándose un breve resumen, una valoración personal y las futuras líneas de trabajo.

Además, se cuenta con 13 Anexos donde se detalla la documentación del SGSI necesaria para la realización del proyecto.

1.3 Definiciones

- **Activo:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- **Alcance:** Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo, si sólo incluye una parte de la organización.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Acción correctiva:** Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI. Aceptación del Riesgo: Decisión de aceptar un riesgo.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

- **Auditoría interna:** Auditoría realizada por la propia organización o en su nombre, para su revisión por la dirección y para otros fines internos, y que podría constituir la base para una autodeclaración de conformidad de la organización

- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- **Apetencia al riesgo:** Nivel y tipo de riesgo que una organización está preparada para aceptar.

- **Apreciación del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo, y evaluación del riesgo.

- **Alerta:** Notificación formal de un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre. Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Control:** Políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados.

- **Continuidad del negocio:** Capacidad de la organización para continuar realizando la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo.

- **Declaración de aplicabilidad:** (del inglés: Statement of Applicability: SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras

el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **Degradación:** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

- **Evidencia:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

- **Impacto:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Incidente de seguridad de la información:** Situación que podría producir o provocar una interrupción, una pérdida, una emergencia o una crisis [ISO / IEC 22301: 2013]

- **No conformidad:** Incumplimiento de un requisito. [ISO / IEC 22301: 2013]

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Salvaguarda:** Procedimiento o mecanismo tecnológico que reduce el riesgo.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

2 Seguridad de la información

La información, como activo de una empresa, es un requerimiento que tiene un valor indispensable para una organización. Se presenta de múltiples formas: en papel, guardada en discos duros o portátiles, subida a la nube, transmitida por correo electrónico...

Debido a la multitud de medios existentes para su divulgación, ésta ha de ser debidamente protegida. Así, la seguridad de la información tiene como objetivo proteger los activos con el fin de garantizar unos niveles adecuados de confidencialidad, integridad y disponibilidad.

2.1 Pilares de la Seguridad de la Información.

Estos tres pilares en los que se basa la seguridad de la información son:

- **Confidencialidad**: Propiedad o requerimiento de la seguridad que exige que la información no puede ser revelada a personas no autorizadas y que no necesiten conocer la información. La pérdida de la confidencialidad puede ocurrir de múltiples maneras, como por ejemplo con la publicación de información confidencial de la organización de manera intencional.
- **Integridad:** Propiedad que garantiza que la información no ha sido modificada por terceros a los que el acceso a la modificación les está restringido.
- **Disponibilidad:** Garantía de que la información sólo es accesible por personal autorizado. Entre los ataques que amenazan la disponibilidad de la información destaca el ataque de denegación del servicio.

A estos tres pilares de la seguridad se pueden añadir otros derivados pero igual de importantes:

- **Autenticidad:** Característica que se refiere a la comprobación y confirmación de la identidad real de los activos y del personal de la organización en todo momento. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.
- **Trazabilidad:** Propiedad por la cual una organización se asegura que en todo momento se podrá determinar quién hizo qué y en qué momento.

2.2 Planos de actuación

Para cumplir con estos principios una organización debe contemplar cuatro planos de actuación:

- **Técnico**: Procedimiento tanto a nivel físico como a nivel lógico.
- **Legal**: Adecuación a la normativa legal presente en determinados sectores de actividad económica.
- **Humano**: Sensibilización y formación de empleados y directivos; definición defunciones y obligaciones del personal.

- **Organizativo**: Definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación

2.3 Ciclo PDCA

El cumplimiento de los pilares de la información lleva a la necesidad de crear un plan de gestión de la seguridad de la información (SGSI) donde se detalle de manera clara y concisa las medidas y acciones que debe aplicar la empresa si quiere estar debidamente protegida así como los documentos que se deberán realizar para la aplicación de éstas.

Para llevar a cabo este plan se usa el denominado “plan PHVA”, (plan PDCA en inglés) instaurado por la ISO 27001, se trata de un ciclo de cuatro fases por las que se tiene que pasar para establecer y gestionar un Sistema de Gestión de la Seguridad.

Estas cuatro fases son:

- **Planificar (“Plan”):** Establecer la política, el alcance, los procedimientos de seguridad que ayudan a gestionar el riesgo y mejorar la seguridad de la información. La finalidad del proceso de planificación es la entrega de resultados acordes con las políticas y los objetivos globales de la organización.
- **Hacer (“Do”):** Se centra en la elaboración e implementación de un plan efectivo a medio y largo plazo que reduzca o evite los posibles riesgos para la Seguridad de la Información. Para ello, se implementa y opera la política y se implantan los controles seleccionados durante el proceso de “planificación
- **Verificar (“Check”):** Los objetivos de esta etapa son:
    - Medir el desempeño de los procesos, es decir, monitorizarlos.
    - Evaluar el cumplimiento de los indicadores establecidos durante el proceso de planificación.
    - Informar sobre los resultados para su revisión.
- **Actuar (“Act”)**: Iniciar acciones correctivas y preventivas en base a los resultados de la auditoría interna del SGSI que garanticen en todo momento la seguridad y protección de la información de la organización. El objetivo de esta fase es lograr la mejora continua del SGSI.

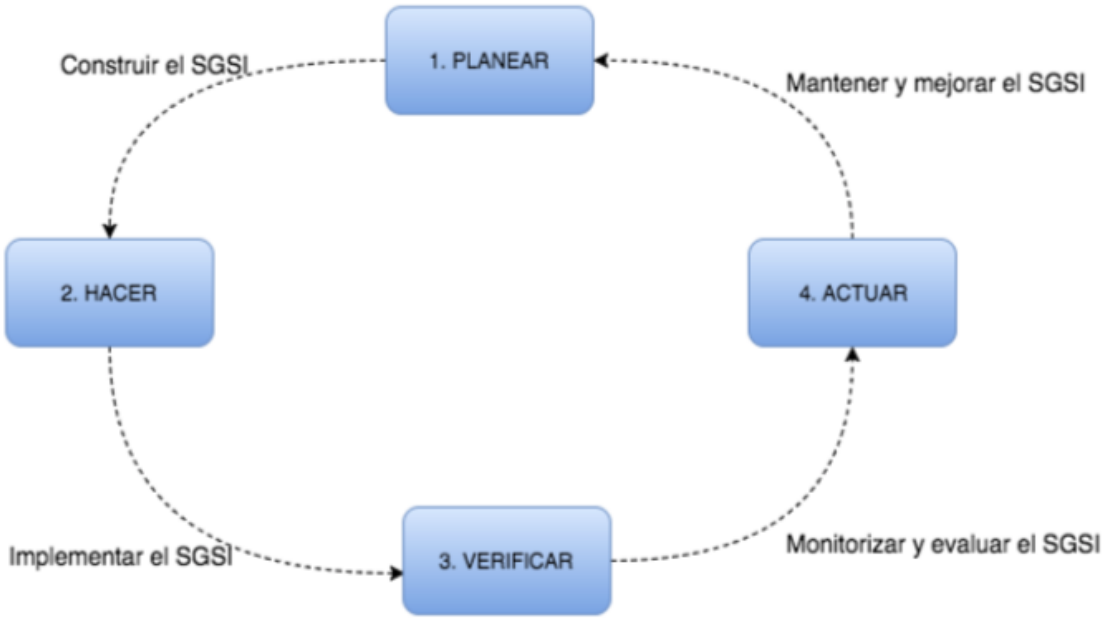


Figura 2: Plan PDCA.

2.4 Estándares de Seguridad de la Información ISO

Los estándares de Seguridad de la Información a partir de los cuales se va a implantar este plan director de seguridad son ISO 27001:2013 e ISO 27002:2013. Éstos son desarrollados por la Organización Internacional de Estándares, ISO (International Standard Organization).

Su origen se remonta al año 1947 cuando representantes de 28 países se juntaron con el objetivo de promover el desarrollo de estándares internacionales para todo tipo de actividades y productos: transporte, medio ambiente, energías...

Sin embargo, no es hasta el año 2000 cuando se crea la necesidad de desarrollar una normativa internacional sobre Seguridad de la información con la creación de la familia de normas 27000, todas ellas basadas en la norma británica (BS) que era la única vigente y que data del año 1995.

Estas normas tienen como objetivo el de ayudar a la empresa a establecer, implementar, monitorizar y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). A continuación se detallan algunas de estas normas:

- **ISO 27001:** “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos”. Especifica los requisitos del plan de gestión de la calidad (PDCA) que está formado por: el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en el contexto de la organización. Esta norma también incluye los requisitos para el análisis y el tratamiento de los riesgos de seguridad de información. La última actualización de esta norma data del 2013.
- **ISO 27002:** “Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información”. Presenta 14 dominios de control que contiene un total de 35 de objetivos de control. La última actualización de esta norma data del 2013.

- **ISO 27003**: ""*Tecnología de la información. Técnicas de seguridad. Guía de implantación de un SGSI*" Proporcionar una guía para la implementación de un SGSI haciendo hincapié en el plan PDCA. La última actualización de esta norma data del 2011.
- **ISO 27004**: "Tecnología de la información. Técnicas de seguridad. Medidas para la Gestión *de la Seguridad".* Especificar las métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles establecidos en la ISO 27001. La última actualización de esta norma data del 2013.
- **ISO 27005:** "*Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en Seguridad de la Información".* Guía de análisis y gestión de los riesgos". Esta norma tiene como objetivo proporcionar una guía para la gestión del riesgo en un Sistema de Gestión de Seguridad de la Información. La última actualización de esta norma data del 2011.
- **ISO 27007:"** Tecnología de la información - Técnicas de seguridad - Directrices para los sistemas *de gestión de seguridad de la información de auditoría***".** Provee una guía para la realización de las auditorías de un Sistema de Gestión de Seguridad de la Información y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.
- **ISO 27017**: Tecnología de la información - Técnicas de seguridad - Controles de seguridad para servicios en la nube**".**Provee una serie de controles basados en la norma ISO 27001 para proveedores y clientes de servicios en la nube.
- **ISO 27018:**Tecnología de la información - Técnicas de seguridad - Requisitos para la protección de la información personal en sistemas cloud**".** Provee una guía a los proveedores de nube pública evaluar riesgos e implementar controles para la protección de los datos personales que tienen almacenados.

A continuación se muestra una imagen de la familia de la ISO 27000:

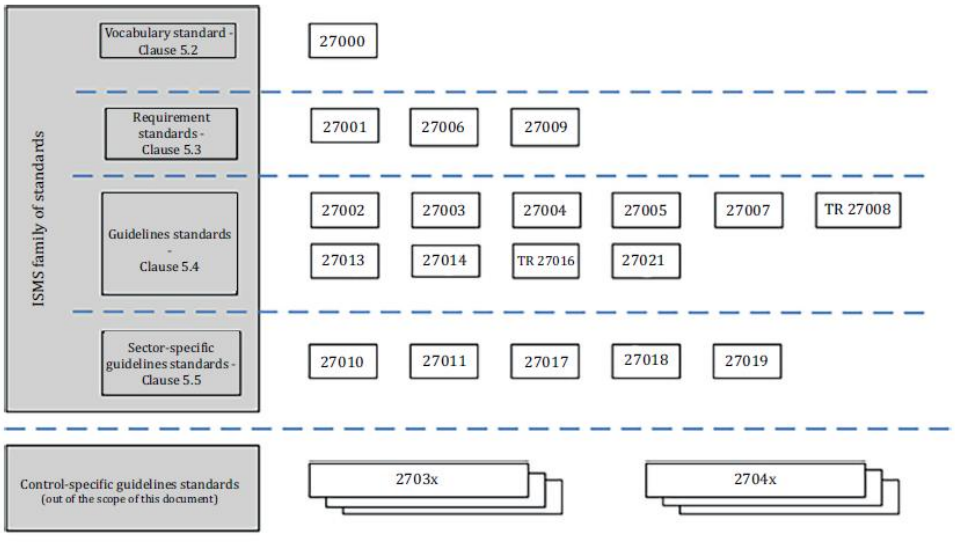


Figura 3: Familia de normas ISO 27000. Copyright 2018 ISO/IEC 27000

3. Situación actual: Contextualización, Objetivos y Análisis Diferencial

3.1 Contextualización

Como se ha comentado durante la primera parte de este trabajo, la empresa para la cual se va a desarrollar el plan director de seguridad es **TrendTip**. TrendTip es una empresa online de moda cuyo objetivo es servir de escaparate a los pequeños comercios textiles y de calzado, haciendo de intermediario entre éstos y sus potenciales compradores. Se trata de una página web donde se muestran las últimas tendencias de moda, mostrando looks completos en los que se mezcla prendas de distintos comercios. En ella, el cliente tiene la opción de hacer clic en las distintas prendas elegidas y ser redirigido a la página web de empresa textil elegida para poder efectuar la compra del producto.

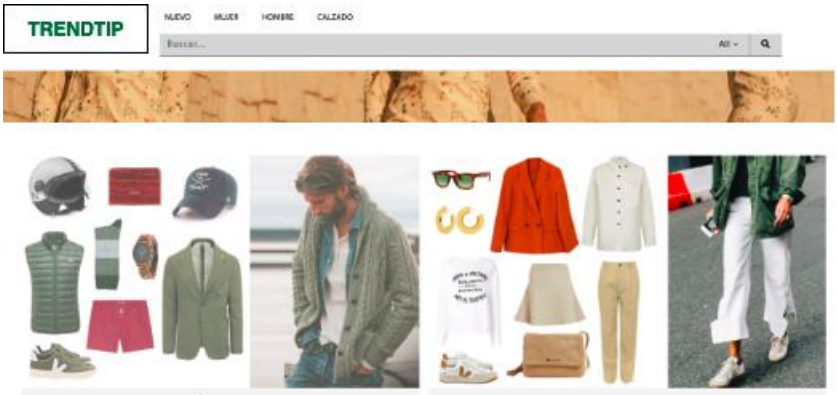


Figura 4: Página web de Trendtip

3.1.1 Ubicación física

La empresa cuenta con una oficina física situada en Madrid. Esta oficina está alojada en un edificio de oficinas que dispone de seguridad las 24 horas al día. Además, la propia oficina cuenta con un sistema de alarma conectada con un sistema de CCTV para prevenir posibles acciones delictivas.

La oficina dispone de:

- una sala de trabajo donde desarrollan sus funciones todos los empleados de la empresa. En ella se ubican todos los puestos de trabajo con sus respectivos ordenadores.
- una sala de reunión: en ella se llevan a cabo las reuniones con proveedores
- una pequeña sala de impresión.

3.1.2 Infraestructura tecnológica

3.1.2.1 Hardware

La organización tiene 4 ordenadores portátiles plataformados para sus cuatro empleados conectados a la red interna de la empresa. La red no está segmentada y sólo cuenta de un dispositivo que hace de router y switch con capacidades de seguridad provistas *as a Service* por el proveedor de servicios de Internet contratado.

3.1.2.2 Software

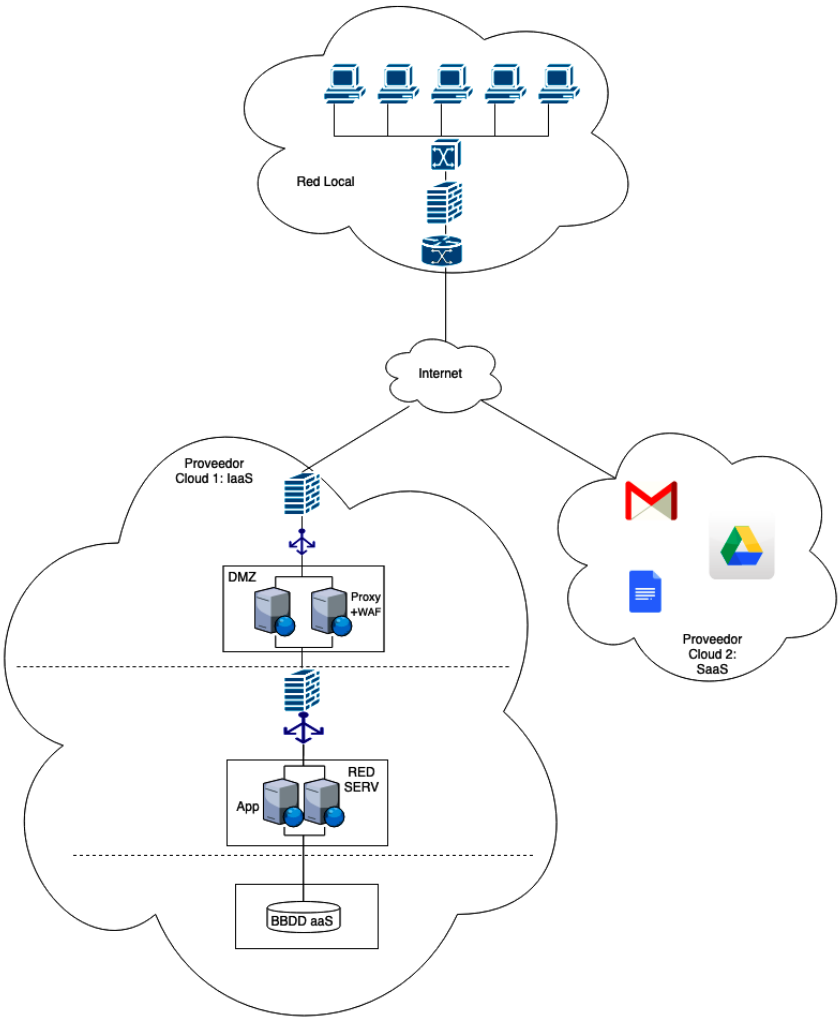
Tres de los cuatro ordenadores disponen de Windows 10, y de licencias de Microsoft Office. El cuarto dispositivo, propiedad del personal encargado de Marketing y Community Manager se trata de un MAC, con SO MacOS Mojave. Este último también dispone de la licencia de Microsoft Office así como la de Adobe Photoshop.

3.1.2.3 Nube

Para asegurar la máxima disponibilidad del servicio se ha contratado dos servicios en la nube:

- IaaS (Infraestructure as a Service): se han contratado dos servidores donde se aloja la página web de la empresa y la base de datos de los proveedores textiles. Se ha diseñado una arquitectura en 3 capas.
- SaaS (Software as a Service): se han contratado servicios en la nube (SaaS) de almacenamiento de documentos y ofimática para toda la gestión estratégica, de recursos humanos y del plan comercial de la empresa.

3.1.2.4 Diagrama de red



3.2. Misión

La misión estratégica de la TrendTip es:

- Servir de referencia a los clientes en cuanto a las últimas tendencias en el sector de la moda.
- Servir de intermediario entre clientes y proveedores de las tendencias.
- Asegurar a sus clientes el más alto grado de integridad, profesionalidad y seguridad.

3.3. Organigrama

Al ser una empresa de reciente creación, la empresa cuenta únicamente con 4 empleados, cuyos roles y responsabilidades se detallan en el siguiente organigrama:

Figura 6: Organigrama TrendTip

- **CEO:** fundador de la empresa y encargado de:
  - Toma de decisiones estratégicas
  - Gestión de Recursos Humanos
  - Gestión de Recursos económicos.
- **Responsable IT**: Se encarga de coordinar todas las actividades de tecnología de la empresa. Entre sus funciones destaca:
  - Administrador de sistemas
  - Responsable de seguridad
  - Analista funcional
  - Arquitecto de sistemas
- **Responsable de Marketing:** Es el encargado de:
  - Gestionar Redes sociales
  - Gestionar acciones publicitarias
- **Responsable de ventas:**
  - Estudiar el mercado en busca de nuevas tendencias
  - Negociar y contratar nuevos proveedores

3.4 Alcance

El sistema de gestión de seguridad de la información a implantar aplica a todos los sistemas que sustentan los siguientes procesos de negocio de la empresa:

1. La página web que hace de intermediaria entre los clientes y los proveedores finales.

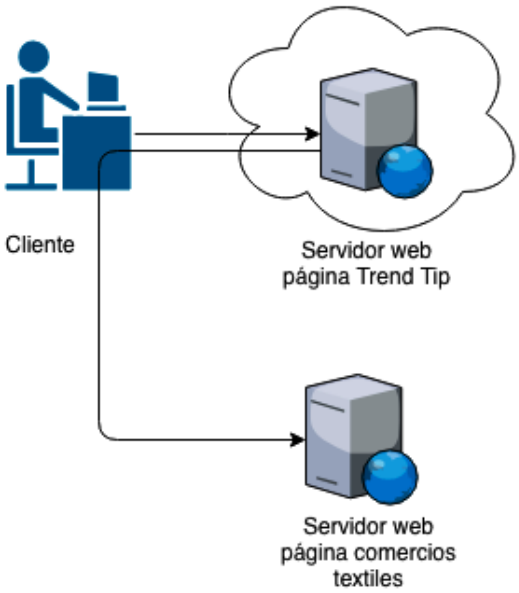


Figura 7: Proceso de intermediación entre clientes y proveedores finales de TrendTip

2. La búsqueda de tendencias y productos para su selección.

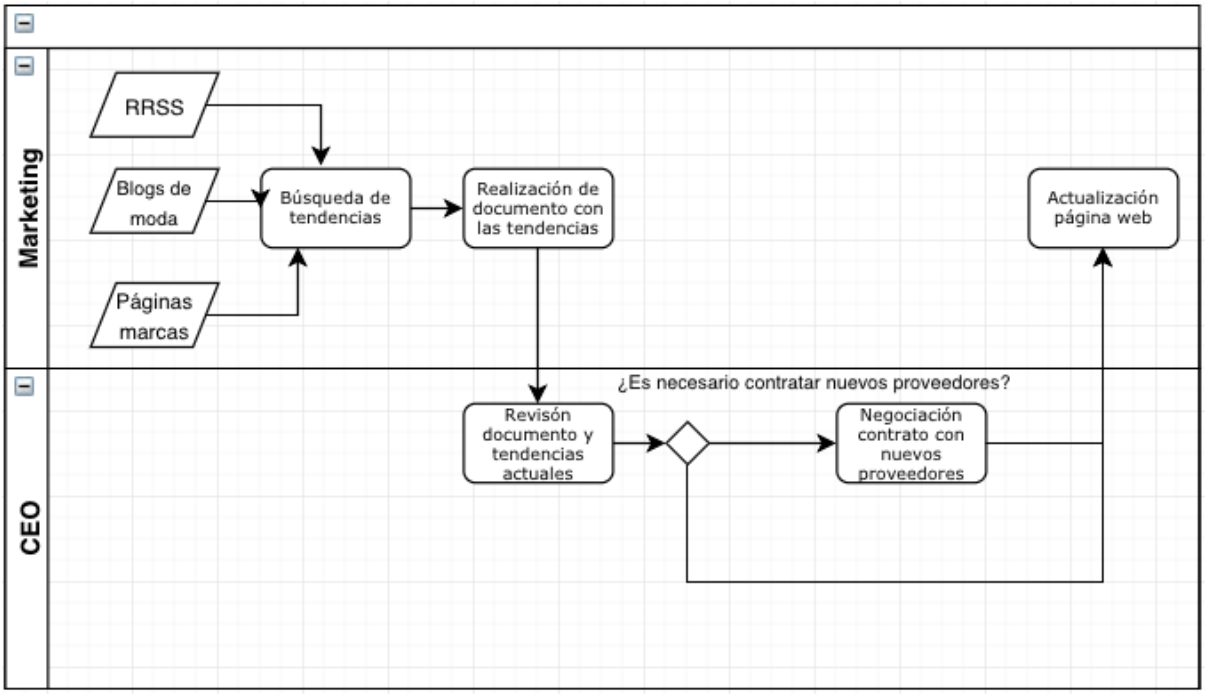


Figura 8: Proceso de búsqueda de tendencias y productos de TrendTip

3.5 Objetivos

TrendTip es una empresa de reciente creación, diseñada para acercar a los consumidores las nuevas tendencias de moda y la posibilidad de hacerse con ella. Debido a la multitud de empresas que existen dedicadas a lo mismo, el directivo de la empresa ha pensado en implantar un Sistema de Gestión de Seguridad de la información para actuar como punto diferenciador frente a otra empresas del mismo sector. Con ello, se pretende:

1. Conseguir un mayor número de visitas y compras a la página web y conseguir los beneficios económicos necesarios para su ampliación de plantilla.
2. Ampliación del número de proveedores partners con los que trabaja para así poder ampliar la oferta a otros sectores como son la cosmética.

3.6 Análisis diferencial

Para establecer el porcentaje de cumplimiento de cada uno de los controles de las normas ISO 27001 e ISO 27002, se tendrán en cuenta los niveles de madurez de procesos establecidos en la norma ISO 21827 y los cuales se describen en la siguiente tabla:

Tabla 2: Niveles de madurez establecidos en la norma ISO 21827

Porcentaje	Criterio	Descripción
0%	Inexistente	No existen controles de seguridad de la información establecidos.
20%	Realizado informalmente	Existen procedimientos para llevar a cabo ciertas acciones en determinado momento. Estas prácticas no se adoptaron formalmente y/o no se les hizo seguimiento y/o no se informaron adecuadamente.
40%	Planificado	Los controles de seguridad de la información establecidos son planificados, implementados y repetibles.
60%	Bien definido	Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización.
80%	Cuantitativamente controlado	Los controles de seguridad de la información están sujetos a verificación para establecer su nivel de efectividad.
100%	Mejora continua	Los controles de seguridad de la información definidos son periódicamente revisados y actualizados. Estos reflejan una mejora al momento de evaluar el impacto.

3.6.1 ISO 27001:2013

Tabla 3: Resultados análisis diferencial ISO 27001

ISO/IEC 27002	Control	Cumplimiento

Tabla 3: Resultados análisis diferencial ISO 27001

4	Contexto de la organización	35 %
5	Liderazgo	67 %
6	Planificación	70 %
7	Soporte	28 %
8	Operación	7 %
9	Evaluación de desempeño	13 %
10	Mejora	20 %

3.6.1.1 Resultados

A continuación se muestran dos gráficos donde se presentan los resultados obtenidos del análisis diferencial. De ellos se evidencia que el cumplimiento de la norma ISO27002 es de un 35%

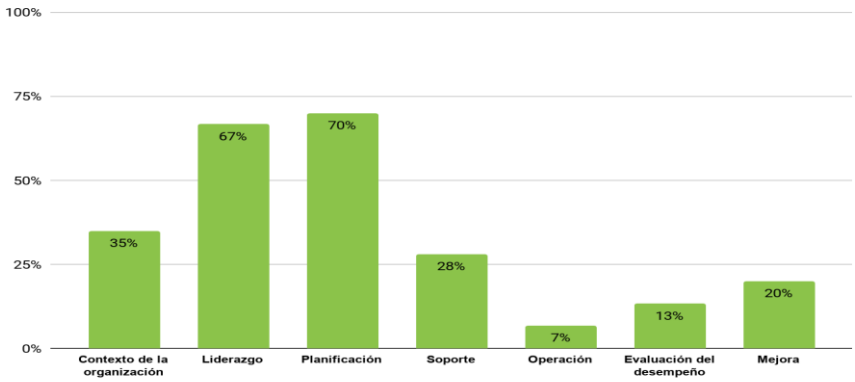


Figura 9: Resultados análisis diferencial ISO 27001

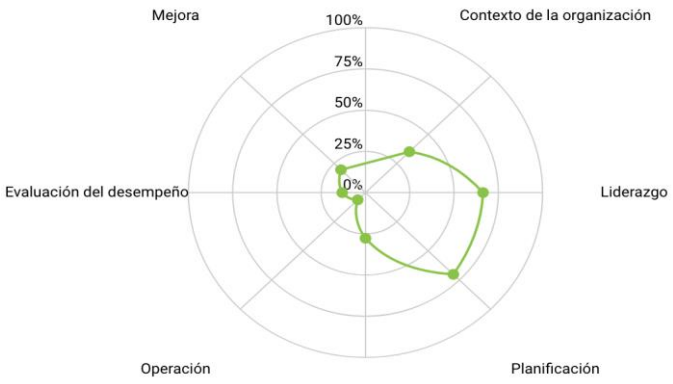


Figura 10: Resultados análisis diferencial ISO 27001

3.6.2 ISO 27002:2013

Tabla 4: Resultados análisis diferencial ISO 27002

ISO/IEC 27002 sección	Control ISO 27002	Cumplimiento
5	Políticas de seguridad de la información	**60 %**
6	Organización	**30 %**
7	Seguridad relativa a los RRHH	**42 %**
8	Gestión de activos	**32 %**
9	Control de acceso	**56 %**
10	Criptografía	**80 %**
11	Seguridad física y del entorno	**53 %**
12	Seguridad de las operaciones	**44 %**
13	Seguridad de las comunicaciones	**64 %**
14	Adquisición, desarrollo y mantenimiento de los sistemas	**50 %**
15	Relación con proveedores	**60 %**
16	Gestión de incidentes	**11 %**
17	Continuidad del negocio	**63 %**
18	Cumplimiento	**53 %**

3.6.1.1 Resultados

A continuación se muestran dos gráficos con los resultados obtenidos del análisis diferencial. De ellos se evidencia que el cumplimiento de la norma ISO27002 es de un 51%

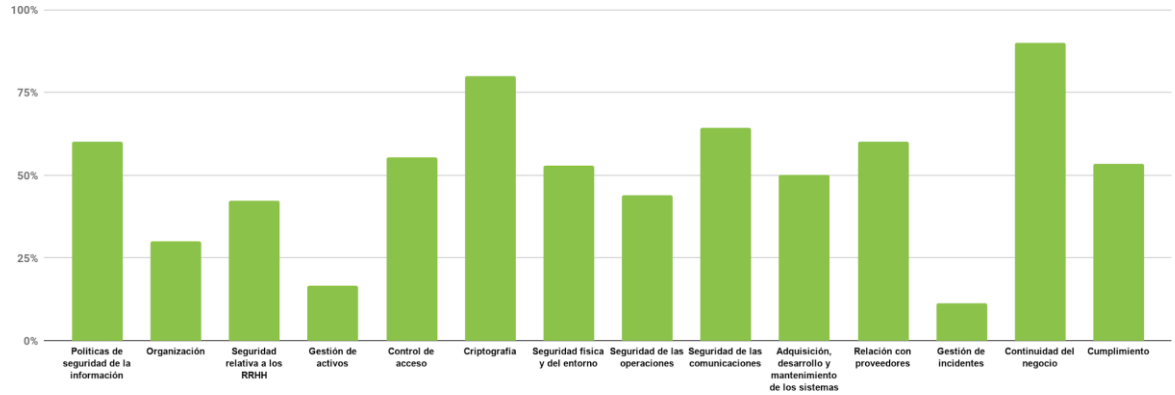


Figura 11: Resultados análisis diferencial ISO 27002

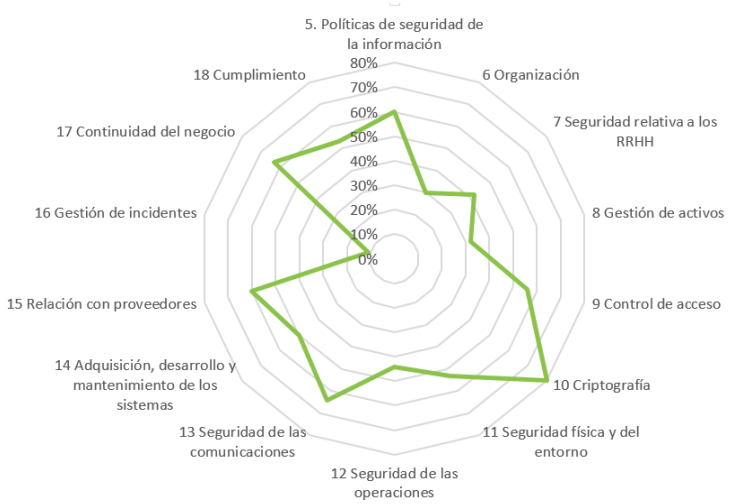


Figura 12: Resultados análisis diferencial ISO 27002

4. Sistema de gestión documental

Todo Sistema de Gestión de Seguridad de la Información debe contar con una serie de documentos, los cuales vienen establecidos en la norma ISO/IEC 27001 y son los que se detallan a continuación:

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento Revisión por Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgos.
- Declaración de Aplicabilidad.

4.1 Política de seguridad

Se trata de uno de los documentos dispuestos en la ISO 27001 como obligatorio. En él se describe toda la normativa interna de la organización. Su finalidad es que todo el personal conozca y cumpla con lo relativo al SGSI implantado.

Además, se detalla qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. Define qué quiere la organización a muy alto nivel, de forma muy general.

El documento de la política de seguridad implementada debe utilizar un lenguaje sencillo y claro que lo pueda comprender todo el personal de la organización.

La Política debe estar completamente actualizada y debe ser revisada anualmente o cuando ocurran alguna de las siguientes situaciones:

- Haya ocurrido algún incidente grave de seguridad.
- Después de una auditoría del sistema fallida
- Haya cambios que afecten a la estructura global de la organización.

En el Anexo B se detalla la política de seguridad implantada así como las políticas específicas que forman parte del cuerpo normativo del SGSI:

- **NT002_Norma de gestión de activos**: Norma que provee las directrices a seguir para la implementación de medidas de seguridad sobre los Sistemas de Información propiedad de TrendTip.
- **NT003_Norma gestión de la continuidad del negocio**
- **NT004_Norma de gestión de incidentes:** Directrices para la actuación contra eventos, incidentes y vulnerabilidades dentro de los Sistemas de Información
- **NT005_Norma de control de acceso**: Norma que establece los criterios mínimos a seguir en materia de control de acceso de usuarios a los Sistemas de Información de TrendTip y la gestión de usuarios, cuentas, privilegios e información de autenticación

- **NT006_Norma de cumplimiento:** Norma que determina los criterios mínimos a seguir referentes al cumplimiento de normativas y regulaciones externas de TrendTip.
- **NT007_Norma de operación:** Establece los criterios de seguridad mínimos a tener en cuenta para la gestión de la operativa de TrendTip.
- **NT008_Norma de gestión de servicios cloud:** Establece las directrices de seguridad a tener cuenta en la gestión y uso de servicios Cloud

4.2 Procedimiento de auditoría interna

Las auditorías internas tienen como misión:

- la revisión de la eficacia y la eficiencia del SGSI: Deben asegurarse que TrendTip está operando de acuerdo a las políticas y procedimientos definidos en el SGSI
- la identificación de los posibles riesgos, vulnerabilidades y debilidades con los que cuenta el SGSI.

El procedimiento de auditoría interna incluye una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), los requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

En el Anexo C se detalla el procedimiento de auditoría interna.

4.3 Gestión de indicadores

Se han establecido una serie de indicadores para medir la eficacia de los controles implantados y el valor objetivo de cada uno de ellos.

En el Anexo D se detalla los indicadores definidos para el sistema de gestión de seguridad de la información de la empresa TrendTip.

4.4 Procedimiento de revisión por la dirección

En el Anexo E se detalla el procedimiento de revisión por la dirección.

4.5 Gestión de roles y responsabilidades

Se han asignado las responsabilidades y los roles basándose en dos puntos fundamentales:

Se han designado las responsabilidades necesarias para asegurar que el Sistema de Gestión de Seguridad de la Información cumple con todos los requisitos de la norma ISO 27001.

Se han designado también las responsabilidades para monitorizar el desempeño del Sistema de Gestión de Seguridad de la Información e informar a la alta dirección.

Más concretamente para TrendTip, se han definido las responsabilidades de las personas que intervienen en el Sistema de gestión de Seguridad de la Información:

- CISO
- Comité de Seguridad

- Auditor interno

En el Anexo F se detalla el procedimiento de revisión por la dirección.

4.6 Metodología de análisis de riesgo

El análisis de riesgos es la acción a través de la cual la organización, mediante el inventario de activos, el alcance y objetivos del SGSI, puede obtener una visión global sobre los riesgos y amenazas a las que se enfrenta. Sus objetivos principales son:

- la identificación de los principales riesgos a los que una entidad está expuesta (fallos en la red, software desactualizado, falta de concienciación...)
- la priorización de las medidas a implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto en caso de producirse.

Para realizar esta evaluación, TrendTip ha seguido la siguiente metodología basada en MAGERIT y que cuyas etapas se detallan a continuación:

1. **Realización de un Inventario de activos**: MAGERIT diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información:
    - Servicios
    - Datos/ información
    - Aplicaciones (Software)
    - Equipos informáticos (Hardware)
    - Personal (interno y externo)
    - Redes de comunicación
    - Soportes de información
    - Equipo auxiliar
    - Instalaciones
2. **Valoración de los activos:** La metodología MAGERIT baraja los dos tipos de valoraciones, cualitativa y cuantitativa. En TrendTip se ha optado por escoger una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en valor monetario su daño o pérdida. En consecuencia la escala se refleja en:

Tabla 5: Valoración cualitativa de los activos

Valoración	Descripción	Valor
Muy alta	>100M euros	10
Alta	<50000 euros	9-7

Tabla 5: Valoración cualitativa de los activos

Media	<10000 euros	6-4
Baja	<5000 euros	3-1
Muy baja	<1000 euros	1

3. **Identificación y valoración de las amenazas**. La siguiente etapa consiste en identificar todas las amenazas a las que los activos identificados se pueden ver expuestos

   Con motivo de la multitud y variedad de amenazas presentes, es imprescindible la experiencia y el conocimiento del activo para identificar de forma correcta y practica aquellas amenazas a las que está expuesto.

   Una vez identificadas las amenazas, se debe establecer la valoración de las amenazas, mediante los siguientes dos parámetros:

   Frecuencia: tiempo de materialización de una amenaza.

Tabla 6: Frecuencia materialización de las amenazas

Frecuencia	Descripción	Valor
Muy alta	una vez al día	100
Alta	una vez a la semana	10
Media	una vez al mes	1
Baja	una vez al año	1/10
Muy baja	una vez cada 10 años	1/100

Degradación: impacto que tiene la materialización de la amenaza en el activo, aplicable a las 5 dimensiones de la seguridad.

Tabla 7: Impacto de las amenazas

Degradación	Descripción	Valor
Muy alta	>100M	5
Alta	<50000 euros	4
Media	<10000 euros	3
Baja	<5000 euros	2
Muy baja	<1000 euros	1

4. **Caracterización de las salvaguardas**.En esta fase se caracterizan las salvaguardas a llevar a cabo para mitigar o reducir el riesgo. Las salvaguardas se pueden clasificar en función de diferentes criterios:
    - Aspecto que se protege (técnico, gestión, personal, físico).
    - Estrategia que adopta la salvaguarda ante el incidente (minimizar, corregir, eliminar, concienciar...).
    - Clase de activo que protege (Equipos hardware, aplicaciones informáticas, personal...).
    - Importancia de la salvaguarda (interesante, importante, muy importante y crítica).
5. **Valoración Impacto y riesgo residual.** El riesgo residual supone el riesgo real al que la entidad está expuesta en el momento de la realización del análisis de riesgo. Es el riesgo sobre el que se deben establecer criterios de aceptación de riesgos y a partir del cual se ha de definir un plan de tratamiento de riesgos para mitigar los riesgos críticos para la entidad.
   Obteniendo los riesgos residuales podremos identificar las principales amenazas a las que se encuentran expuestos los activos y que pueden tener un mayor impacto en los principales servicios ofrecidos o en la información en caso de materializarse. Disponer de una visión clara de las mismas nos permite enfocar de un modo adecuado los recursos disponibles para gestionar la seguridad de la información.

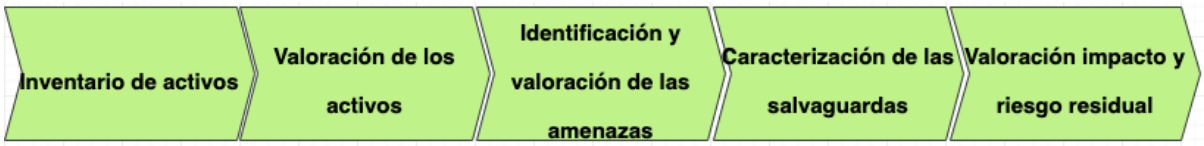


Figura 13: Etapas metodología análisis de riesgo MAGERIT

4.7 Declaración de aplicabilidad

La declaración de aplicabilidad es uno de los documentos más importantes del Sistema de Gestión de Seguridad de la Información y requisito de documentación del estándar ISO 27001. Esto se debe a que es el paso intermedio entre las evaluación de riesgos y el tratamiento de ellos.

Este documento incluye:

- Lista los controles de seguridad a aplicar, tanto los definidos en la ISO 27002 como aquellos que se consideren oportunos, y la justificación de su implantación o exclusión.
- La lista de controles en proceso de implantación
- La lista de controles ya implantados.

En el Anexo G se detalla el la declaración de aplicabilidad de TrendTip

5. Análisis de riesgos

5.1 Introducción

Para llevar a cabo la implementación de un Sistema de Gestión de Seguridad es crucial la realización de un análisis de riesgos. El análisis de los riesgos permite determinar cuáles son los factores de riesgo que tendrían un mayor impacto sobre nuestra organización y, por tanto, cuáles de esos activos deben ser gestionados con especial atención.

Para realizar este análisis se ha optado, como se ha definido en el documento "Metodología de análisis de riesgo", por MAGERIT (acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) elaborada por el Consejo Superior de Administración Electrónica de España.

MAGERIT está destinada para todas aquellas organizaciones que trabajan con información digital y sistemas de información. Permite saber qué y cuánto está en juego y ayudar a protegerlo. Su finalidad es conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos.

MAGERIT persigue los siguientes objetivos:

- Concienciar de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos.
- Efectuar un tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

5.2 Inventario de activos

De acuerdo a la metodología establecida, el primer paso para realizar una análisis de riesgos es analizar los activos que están vinculados a la información.

Se define Activo como: "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos". [UNE 71504:2008]

Acorde a la metodología MAGERIT los activos se dividen en los siguientes grupos:

- **Instalaciones:** Lugares donde se hospedan los sistemas de información
- **Hardware:** Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
- **Aplicación:** Programas, aplicativos, desarrollos, etc.
- **Datos:** Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.

- **Red:** Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
- **Servicios:** Función que satisface una necesidad de los usuarios.
- **Equipamiento auxiliar:** Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
- **Personal:** Personal relacionado con los sistemas de información.

En el anexo H se muestra una tabla con el inventario de activos de TrendTip clasificados según los grupos definidos en la metodología MAGERIT

5.3 Valoración de los activos

Una vez clasificados e identificados los activos de la organización, debemos determinar el valor de estos activos con el fin de aplicar una serie de medidas que garanticen que se encuentran correctamente protegidos.

MAGERIT en su Libro II (punto 2.1) propone una valoración de los activos en base a las siguientes categorías:

- Muy alto
- Alto
- Medio
- Bajo
- Muy bajo

A continuación, se muestra una tabla con la valoración del activo en función de su impacto económico:

Tabla 8: Valoración del activo en función del impacto económico

Valoración	Descripción
Muy alta	>100M euros
Alta	<50000 euros
Media	<10000 euros
Baja	<5000 euros
Muy baja	<1000 euros

5.4 Dimensiones de los activos

Una vez identificados los activos, debe realizarse la valoración ACIDT de los mismos. Dicha valoración mide la criticidad de los activos en función de las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio:

- **Autenticidad [A]:** El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.
- **Confidencialidad [C]:** El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.
- **Integridad [I]:** El nivel de seguridad requerido en el aspecto de integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información
- **Disponibilidad [D]:**El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.
- **Auditabilidad/Trazabilidad [T]:** El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.

Esta valoración permite a posteriori valorar el impacto que puede tener la materialización de una amenaza sobre la parte de activo expuesto.

En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios por cada una de las dimensiones. En el anexo I se puede ver la valoración de cada una de las dimensiones en los activos

Tabla 9: Escala de valoración de la confidencialidad

[Confidencialidad]:Valor	Descripción
[C]:10	- porque la información debe conocerla un número muy reducido de personas - por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su revelación causaría un grave daño, de imposible reparación - porque su revelación supondría el incumplimiento de una norma - porque su revelación causaría pérdidas económicas muy elevadas o alteraciones financieras significativas
[C]:7-9	- porque la información debe conocerla un número reducido de personas - por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su revelación causaría un grave daño, de difícil o imposible reparación - porque su revelación supondría el incumplimiento grave de una norma

Tabla 9: Escala de valoración de la confidencialidad

	- porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
[C]:4-6	- porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita - por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su revelación causaría un daño importante aunque subsanable - porque su revelación supondría el incumplimiento material o formal de una norma - porque su revelación causaría pérdidas económicas importantes
[C]:1-3	- porque la información no deben conocerla personas ajenas a la organización - por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su revelación causaría algún perjuicio - porque su revelación supondría el incumplimiento leve de una norma - porque su revelación supondría pérdidas económicas apreciables
[C]:0	- información de carácter público, accesible por cualquier persona

Tabla 10: Escala de valoración de la disponibilidad

[Disponibilidad]:Valor	Descripción
[D]:10	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la indisponibilidad de la información causaría un daño de difícil reparación - porque la indisponibilidad de la información supondría el incumplimiento muy grave de una norma - porque la indisponibilidad de la información causaría un daño reputacional muy grave - cuando el RTO es inferior a 4 horas
[D]:7-9	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la indisponibilidad de la información causaría un grave daño - porque la indisponibilidad de la información supondría el incumplimiento grave de una norma - porque la indisponibilidad de la información causaría un daño reputacional grave - cuando el RTO es inferior a 8 horas

Tabla 10: Escala de valoración de la disponibilidad

[D]:4-6	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la indisponibilidad de la información causaría un daño subsanable - porque la indisponibilidad de la información supondría el incumplimiento formal de una norma - porque la indisponibilidad de la información causaría un daño reputacional importante - cuando el RTO se sitúa entre 8 y 24 horas (un día)
[D]:1-3	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la indisponibilidad de la información causaría algún perjuicio - porque la indisponibilidad de la información supondría el incumplimiento leve - porque la indisponibilidad de la información causaría un daño reputacional apreciable - cuando el RTO se sitúa entre 1 y 5 días (una semana)
[D]:0	- cuando la información es prescindible por tiempo indefinido - cuando el RTO es superior a una semana

Tabla 11: Escala de valoración de la autenticidad

[Autenticidad] : Valor	**Descripción**
[A]:10	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la falsedad en su origen o en su destinatario causaría un grave daño, de imposible reparación - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas muy elevadas - porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave
[A]:7-9	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la falsedad en su origen o en su destinatario causaría un grave daño, de imposible reparación - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas muy elevadas - porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave

Tabla 11: Escala de valoración de la autenticidad

[A]:4-6	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes - porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante
[A]:1-3	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la falsedad en su origen o en su destinatario causaría algún perjuicio - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas apreciables - porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable
[A]:0	- cuando el origen es irrelevante o ampliamente conocido por otros medios - cuando el destinatario es irrelevante

Tabla 12: Escala de valor por la trazabilidad

[Trazabilidad]: Valor	Descripción
[T]:10	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error grave - porque la incapacidad para rastrear un acceso a la información dificultaría enormemente la capacidad para perseguir delitos
[T]:7-9	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad de subsanar un error grave - porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[T]:4-6	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error importante - porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos

Tabla 12: Escala de valor por la trazabilidad

[T]:1-3	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores - porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos
[T]:0	- cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios - cuando no se pueden perpetrar delitos relevante, o su investigación es fácilmente realizable por otros medios

Tabla 13: Escala de valoración por su integridad

[Integridad]:Valor	Descripción
[I]:10	- por disposición legal o administrativa - porque su manipulación o modificación no autorizada causaría un daño de imposible reparación - porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas
[I]:7-9	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su manipulación o modificación no autorizada causaría un grave daño, de difícil reparación - porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas - porque su manipulación o alteración no autorizada causaría un daño reputacional grave
[I]:4-6	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable - porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma - porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes - porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

Tabla 13: Escala de valoración por su integridad

[I]:1-3	- por disposición legal o administrativa: ley, decreto, orden, reglamento, … - porque su manipulación o modificación no autorizada causaría algún perjuicio - porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma - porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables - porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable
[I]:0	- cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables

5.5 Tabla resumen de la valoración

De forma resumida, lo visto hasta ahora nos permite generar una tabla donde reflejaremos tanto la valoración de activos como los aspectos críticos del mismo

Tabla 14: Valoración de activos

Ámbito	Activo	Valor	Aspectos críticos				
			[A]	[C]	[I]	[D]	[T]
Instalaciones	Oficina	Medio	3	7	5	7	7
Hardware	Ordenadores personales x 3	Medio	4	5	5	4	4
Hardware	Ordenador	Bajo	3	4	3	3	3
Hardware	Impresora	Bajo	4	3	4	3	3
Hardware	Teléfonos x 4	Medio	4	4	5	6	4
Hardware	Cámara fotográfica	Bajo	4	5	5	4	1
Hardware	Router	Bajo	2	2	2	1	1
Hardware	Switch	Bajo	3	2	2	2	1
Hardware	Firewall	Muy bajo	1	1	1	1	1
Aplicación	Máquina virtual RedHat x2	Alto	6	9	8	10	6
Aplicación	Windows Profesional 10	Bajo	2	1	1	6	4

Tabla 14: Valoración de activos

Aplicación	MACos Mojave	Bajo	2	1	1	6	4
Aplicación	Adobe Photoshop	Bajo	1	1	1	1	1
Aplicación	Java Enterprise	Bajo	4	4	3	4	3
Aplicación	Antivirus	Muy bajo	1	1	1	1	1
Aplicación	Microsoft Office	Muy bajo	1	1	1	1	1
Aplicación	Servidor web x2	Alto	4	2	7	10	9
Datos	Código fuente	Alto	9	8	10	7	9
Datos	Contratos con proveedores	Muy alto	10	10	10	8	8
Datos	BBDD de clientes	Muy alto	10	10	10	5	8
Datos	BBDD empleados	Alto	9	10	9	4	9
Datos	BBDD aplicación	Alto	7	4	10	10	7
Datos	Contenido audiovisual	Medio	5	8	7	5	5
Datos	Resultados análisis de tendencias	Alto	8	9	7	7	8
Datos	Copias de respaldo de la BBDD	Muy alto	9	9	9	10	8
Datos	Ficheros configuración de los sistemas	Alto	8	10	10	8	8
Datos	Logs de acceso a los sistemas	Alto	9	7	10	8	9
Red	Red Local	Medio	5	8	7	5	5
Servicio	Servicio de proveedor de servicios SaaS	Alto	8	8	10	8	8
Servicio	Servicio de BBDD como servicio	Alto	6	6	10	10	10
Servicio	Servicio de proveedor de servicios IaaS	Muy alto	10	10	10	10	10
Equipamiento auxiliar	Sistemas de alimentación	Bajo	2	4	3	4	3
Equipamiento auxiliar	CCTV	Muy bajo	1	1	1	1	1

Tabla 14: Valoración de activos

Equipamiento auxiliar	Equipos de climatización	Muy bajo	1	1	1	1	1
Personal	CEO	Alto	9	9	9	9	9
Personal	Responsable IT	Alto	9	8	7	8	9
Personal	Responsable de marketing	Medio	7	7	7	7	7
Personal	Responsable de ventas	Medio	7	7	7	7	7

5.6 Análisis de las amenazas

Una vez identificados y evaluados los activos, el siguiente paso es evaluar a qué amenazas están expuestos estos activos, con qué frecuencia se materializan y cómo éstas pueden afectar a los distintos aspectos de la seguridad.

Se denomina amenaza a toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Acorde a la metodología MAGERIT (libro II, capítulo 5), las amenazas se pueden clasificar en los siguientes bloques:

- **Desastres naturales**: sucesos que ocurren sin la intervención del ser humano (incendios, inundaciones, terremotos...)
- **De origen industrial**: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana (explosiones, sobrecarga eléctrica)
- **Errores y fallos no intencionados:** Fallos no intencionales causados por las personas
- **Ataques intencionados:** Fallos deliberados causados por las personas

La frecuencia de las amenazas se ha valorado según la siguiente tabla:

Tabla 15: Frecuencia materialización de las amenazas

Frecuencia	Descripción	Valor
Muy alta	una vez al día	100
Alta	una vez a la semana	10
Media	una vez al mes	1
Baja	una vez al año	1/10
Muy baja	una vez cada 10 años	1/100

En el anexo I se muestran una serie de tablas donde se ha analizado la frecuencia con que puede producirse la amenaza por cada activo, así como su impacto en las distintas dimensiones de la seguridad.

5.7 Impacto potencial

Una vez analizado el impacto de las amenazas en las distintas dimensiones de seguridad, y dado que conocemos los valores de los diferentes activos, podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Así pues, definimos impacto potencial:

Impacto potencial = valor del activo * impacto materialización de la amenaza

Tabla 16: Impacto potencial

Activo	Valor activo					Impacto materialización					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Oficina	3	7	5	7	7			50%	100%		0	0	2,5	7	0
Ordenadores personales x 3	4	5	5	4	4		100%	100%	100%		0	5	5	0	0
Ordenador	3	4	3	3	3		100%	100%	100%		0	4	3	3	0
Impresora	4	3	4	3	3		100%	100%	100%		0	3	4	3	0
Teléfonos x 4	4	4	5	6	4		100%	100%	100%		0	4	5	6	0
Cámara fotográfica	4	5	5	4	1		100%	100%	100%		0	5	5	4	0
Router	2	2	2	1	1		100%	100%	100%		0	2	2	1	0
Switch	3	2	2	2	1		100%	100%	100%		0	2	2	2	0
Firewall	1	1	1	1	1		100%	100%	100%		0	1	1	1	0
Máquina virtual RedHat x2	6	9	8	10	6	100%	100%	100%	100%		6	9	8	10	0
Servidor web x2	4	2	7	10	9	100%	100%	100%	100%		4	2	7	10	0
Windows Profesional 10	2	1	1	6	4	100%	100%	100%	100%		2	1	1	6	0
MACos Mojave	2	1	1	6	4	100%	100%	100%	100%		2	1	1	6	0

Tabla 16: Impacto potencial

Adobe Photoshop	1	1	1	1	1	100%	100%	100%	100%		1	1	1	1	0
Java Enterprise	4	4	3	4	3	100%	100%	100%	100%		4	4	3	4	0
Antivirus	1	1	1	1	1	100%	100%	100%	100%		1	1	1	1	0
Microsoft Office	1	1	1	1	1	100%	100%	100%	100%		1	1	1	1	0
Código fuente	9	8	10	7	9	100%	100%	100%	100%		9	8	10	7	0
Contratos con proveedores	10	10	10	8	8	100%	100%	100%	100%		10	10	10	8	0
BBDD de clientes	10	10	10	5	8	100%	100%	100%	100%		10	10	10	5	0
BBDD empleados	9	10	9	4	9	100%	100%	100%	100%		9	10	9	4	0
BBDD aplicación	7	4	10	10	7	100%	100%	100%	100%		7	4	10	10	0
Contenido audiovisual	5	8	7	5	5	100%	100%	100%	100%		5	8	7	5	0
Resultados análisis de tendencias	8	9	7	7	8	100%	100%	100%	100%		8	9	7	7	0
Copias de respaldo de la BBDD	9	9	9	10	8	100%	100%	100%	100%		9	9	9	10	0
Ficheros configuración de los sistemas	8	10	10	8	8	100%	100%	100%	100%		8	10	10	8	0
Logs de acceso a los sistemas	9	7	10	8	9	100%	100%	100%	100%		9	7	10	8	0
Red Local	5	8	7	5	5			100%	100%	100%	0	0	7	5	5
Servicio de proveedor de servicios SaaS	8	8	10	8	8		100%	100%	100%	100%	0	8	10	8	8
Servicio de proveedor de servicios IaaS	10	10	10	10	10		100%	100%	100%	100%	0	10	10	10	10
Servicio de BBDD como servicio	6	6	10	10	10		100%	100%	100%	100%	0	6	10	10	10
Sistemas de alimentación	2	4	3	4	3		20%	10%	100%	100%	0	0,8	0,3	4	3
CCTV	1	1	1	1	1		20%	10%	100%	100%	0	0,2	0,1	1	1
Equipos de climatización	1	1	1	1	1		20%	10%	100%	100%	0	0,2	0,1	1	1
CEO	9	9	9	9	9	50%	50%	50%	100%	50%	4,5	4,5	4,5	9	4,5

Tabla 16: Impacto potencial

Responsable IT	9	8	7	8	9	50%	50%	50%	100%	50%	4,5	4	3,5	8	4,5
Responsable de marketing	7	7	7	7	7	50%	50%	50%	100%	50%	3,5	3,5	3,5	7	3,5
Responsable de ventas	7	7	7	7	7	50%	50%	50%	100%	50%	3,5	3,5	3,5	7	3,5

5.8 Nivel de Riesgo Aceptable y riesgo Residual

Por último, debemos calcular el nivel de riesgo al que está expuesta la organización. Para ello definiremos el riesgo como:

Riesgo = Impacto potencial * Frecuencia materialización de la amenaza

Una vez calculado, es necesario definir un límite a partir del cual podamos decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar controles.

La organización ha decidido definir el umbral del riesgo en 9. Este nivel de riesgo aceptable se encuentra aprobado por la Dirección, y se tienen que definir los criterios para establecer dicho nivel.

Por otra parte, una vez establecido el control, se reducirá el riesgo, pero este seguirá existiendo (lo deseable es conseguir reducirlo para que esté por debajo del nivel aceptable), a este riesgo que seguirá existiendo después de aplicar los controles de seguridad, se denomina riesgo residual.

Tabla 16: Riesgo de los activos

Activo	**Impacto potencial**					**Frecuencia amenaza**	**Riesgo**				
	[A]	**[C]**	**[I]**	**[D]**	**[T]**		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Oficina	0	0	2,5	7	0	0,1	0	0	0,25	0,7	0
Ordenadores personales x 3	0	5	5	0	0	1	0	5	5	0	0
Ordenador	0	4	3	3	0	1	0	4	3	3	0
Impresora	0	3	4	3	0	1	0	3	4	3	0

Tabla 16: Riesgo de los activos

Teléfonos x 4	0	4	5	6	0	1	0	4	5	6	0
Cámara fotográfica	0	5	5	4	0	1	0	5	5	4	0
Router	0	2	2	1	0	1	0	2	2	1	0
Switch	0	2	2	2	0	1	0	2	2	2	0
Firewall	0	1	1	1	0	1	0	1	1	1	0
Máquina virtual RedHat x2	6	9	8	10	0	1	6	9	8	10	0
Servidor web x2	4	2	7	10	0	10	40	20	70	100	0
Windows Profesional 10	2	1	1	6	0	1	2	1	1	6	0
MACos Mojave	2	1	1	6	0	1	2	1	1	6	0
Adobe Photoshop	1	1	1	1	0	0,1	0,1	0,1	0,1	0,1	0
Java Enterprise	4	4	3	4	0	0,1	0,4	0,4	0,3	0,4	0
Antivirus	1	1	1	1	0	0,1	0,1	0,1	0,1	0,1	0
Microsoft Office	1	1	1	1	0	1	1	1	1	1	0
Código fuente	9	8	10	7	0	10	90	80	100	70	0
Contratos con proveedores	10	10	10	8	0	10	100	100	100	80	0
BBDD de clientes	10	10	10	5	0	10	100	100	100	50	0
BBDD empleados	9	10	9	4	0	1	9	10	9	4	0
BBDD aplicación	7	4	10	10	0	10	70	40	100	100	0
Contenido audiovisual	5	8	7	5	0	10	50	80	70	50	0
Resultados análisis de tendencias	8	9	7	7	0	10	80	90	70	70	0
Copias de respaldo de la BBDD	9	9	9	10	0	10	90	90	90	100	0
Ficheros configuración de los sistemas	8	10	10	8	0	10	80	100	100	80	0
Logs de acceso a los sistemas	9	7	10	8	0	10	90	70	100	80	0
Red Local	0	0	7	5	5	10	0	0	70	50	50

Tabla 16: Riesgo de los activos

Servicio de proveedor de servicios SaaS	0	8	10	8	8	0,1	0	0,8	1	0,8	0,8
Servicio de proveedor de servicios IaaS	0	10	10	10	10	0,1	0	1	1	1	1
Servicio de BBDD como servicio	0	6	10	10	10	0,1	0	0,6	1	1	1
Sistemas de alimentación	0	0,8	0,3	4	3	0,1	0	0,08	0,03	0,4	0,3
CCTV	0	0,2	0,1	1	1	0,1	0	0,02	0,01	0,1	0,1
Equipos de climatización	0	0,2	0,1	1	1	0,1	0	0,02	0,01	0,1	0,1
CEO	4,5	4,5	4,5	9	4,5	1	4,5	4,5	4,5	9	4,5
Responsable IT	4,5	4	3,5	8	4,5	1	4,5	4	3,5	8	4,5
Responsable de marketing	3,5	3,5	3,5	7	3,5	1	3,5	3,5	3,5	7	3,5
Responsable de ventas	3,5	3,5	3,5	7	3,5	1	3,5	3,5	3,5	7	3,5

6. Propuesta de proyectos

6.1 Introducción

A partir de los resultados obtenidos del análisis de riesgos efectuado en el apartado anterior, se han definido una serie de proyectos para ayudar a TrendTip a mitigar el riesgo actual al que está expuesta la organización y evolucionar el cumplimiento de la ISO hasta un nivel adecuado.

Dichos proyectos son el resultado de agrupar un conjunto de recomendaciones identificadas en la fase de análisis de riesgos para facilitar su ejecución.

Los proyectos están cuantificados económicamente y se encuentran planificados en el tiempo. Cada uno de los proyectos se ha dividido en fases de implantación y éstas se muestran, por cada proyecto, en un diagrama de Gantt.

Para el cálculo del coste que supone cada proyecto, se ha procedido a sumar el coste que tendría los honorarios del personal externo que ejecuta el proyecto, así como, en caso de que fuera necesario, el coste del hardware o software requerido para llevar a cabo el proyecto.

La consecución de estos objetivos está pensada para que se realice durante el año en curso. Cabe destacar que debido al pequeño tamaño de la empresa, se han elegido proyectos de

corta duración y que no supongan un grave esfuerzo económico para la empresa y los empleados que deban ejecutar dichos proyectos.

6.2. Propuestas

Tal y como se puede observar en la tabla del apartado anterior, 5.8, hay 3 categorías de activos para los que se requiere la ejecución de proyectos para reducir el riesgo al que están sometidos:

- Datos
- Red
- Servidores
- Personal

Los activos más vulnerables, aquellos que cuentan con mayor scoring de riesgo son los **datos.** Esto se debe principalmente a que se trata de un activo crítico, pues sustenta la base del negocio de TrendTip. Para reducir los riesgos derivados de estos activos se han propuesto los siguientes proyectos:

- Proyecto 1: Plan de continuidad del negocio
- Proyecto 2: Política de backups
- Proyecto 3: Plan de concienciación y formación en materia de seguridad
- Proyecto 4: Plan de control de cambios
- Proyecto 5: Anonimización de la base de datos
- Proyecto 6: Plan de gestión de incidentes

Sin embargo, no sólo los datos tienen un perfil de riesgo alto, otros de los activos para los que la organización considera conveniente realizar proyectos para reducir el nivel de riesgo son: el servidor web y la máquina virtual de redHat y la red lan. Para ello, el proyecto propuesto es:

- Proyecto 7: Implementación de un sistema de monitorización

Por último, se encuentra el personal empleado:

- Proyecto 8: Proceso de gestión del conocimiento

En el anexo J, se muestra en detalle cada uno de estos proyectos (objetivo, descripción, planificación, personal, riesgos a mitigar y beneficios de su implantación).

A continuación se muestra un resumen de todos los proyectos ejecutados, con su duración y coste adicional así como diagrama de Gantt con la planificación de todos los proyectos a ejecutar:

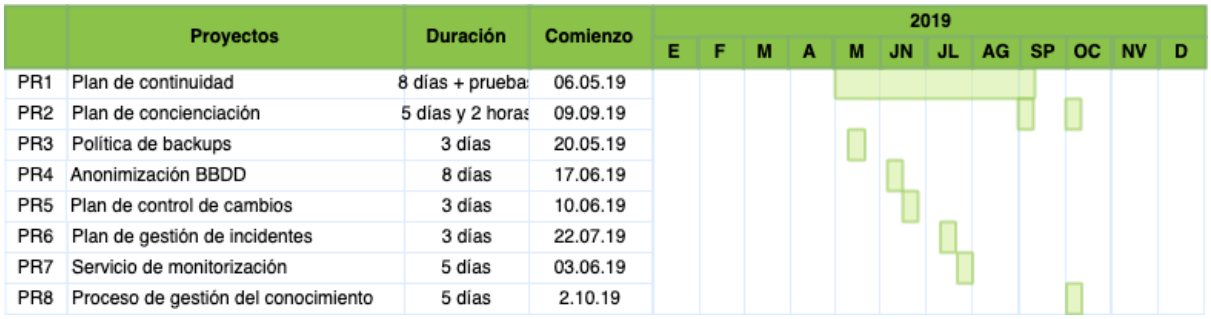


Figura 14: Diagrama de Gantt de proyectos

Tabla 18: Resumen proyectos ejecutados

Proyecto	Control ISO asociado	Duración	Coste adicional
Plan de continuidad	A.17: Aspectos de seguridad de la información para la gestión de la continuidad del negocio	7 días + cursos	3100 euros
Plan de concienciación	A7.2: Seguridad relativa a los RRHH	5 días	1200 euros
Política de backups	A12.3 Copias de seguridad	3 días	No tiene coste adicional. El trabajo es realizado por el responsable TI de la empresa durante su jornada laboral
Plan de control de cambios	A 12.1.2: Gestión de cambios	3 días	No tiene coste adicional. El trabajo es realizado por el responsable TI de la empresa durante su jornada laboral
Anonimización BBDD	A.10. Criptografía	2 días	1200 euros
Plan de gestión de incidentes	A.16: Gestión de incidentes de seguridad de la información	3 días	No tiene coste adicional. El trabajo es realizado por el responsable TI de la empresa durante su jornada laboral
Plan de gestión de cambios	A 10.5 Copias de seguridad	3 días	No tiene coste adicional. El trabajo es realizado por el responsable TI de la empresa durante su jornada laboral
Implementación de servicio monitorización	A.12: Seguridad de las operaciones A.14: Adquisición, desarrollo y mantenimiento de los procesos de soporte	5 días	1600 euros

Tabla 18: Resumen proyectos ejecutados

Proceso de gestión de conocimiento	A15.Relación con proveedores, A.6 Organización de la seguridad de la información A.8 Gestión de activos	5 días	1200 euros

6.3 Resultados

Los proyectos planteados ayudan a la mejora del riesgo de la Organización, haciendo que evolucione el riesgo positivamente. Esto se debe a que las medidas planteadas ayudan a reducir el impacto potencial sobre los activos y la frecuencia de materialización de las amenazas.

En la tabla que se muestra a continuación, se detalla la evolución del riesgo y del impacto de cada uno de los activos:

Tabla 19: Riesgo de los activos tras la ejecución de los proyectos planteados

Activo	**Impacto potencial**					**Frecuencia amenaza**	**Riesgo**				
	[A]	**[C]**	**[I]**	**[D]**	**[A]**		**[A]**	**[C]**	**[I]**	**[D]**	**[A]**
Oficina	0	0	2,5	7	0	0,1	0	0	0,25	0,7	0
Ordenadores personales x 3	0	5	5	0	0	1	0	5	5	0	0
Ordenador	0	4	3	3	0	1	0	4	3	3	0
Impresora	0	3	4	3	0	1	0	3	4	3	0
Teléfonos x 4	0	4	5	6	0	1	0	4	5	6	0
Cámara fotográfica	0	5	5	4	0	1	0	5	5	4	0
Router	0	2	2	1	0	1	0	2	2	1	0
Switch	0	2	2	2	0	1	0	2	2	2	0
Firewall	0	1	1	1	0	1	0	1	1	1	0
Máquina virtual RedHat x2	6	9	8	5	0	0,1	0,6	0,9	0,8	0,5	0
Servidor web x2	4	2	7	5	0	1	4	2	7	5	0
Windows Profesional 10	2	1	1	6	0	1	2	1	1	6	0
MACos Mojave	2	1	1	6	0	1	2	1	1	6	0
Adobe Photoshop	1	1	1	1	0	0,1	0,1	0,1	0,1	0,1	0

Tabla 19: Riesgo de los activos tras la ejecución de los proyectos planteados

Java Enterprise	4	4	3	4	0	0,1	0,4	0,4	0,3	0,4	0
Antivirus	1	1	1	1	0	0,1	0,1	0,1	0,1	0,1	0
Microsoft Office	1	1	1	1	0	1	1	1	1	1	0
Código fuente	6	8	5	7	0	1	6	8	5	7	0
Contratos con proveedores	5	10	5	5	0	1	5	10	5	5	0
BBDD de clientes	5	5	7	4	0	0,1	0,5	0,5	0,7	0,4	0
BBDD empleados	5	5	7	4	0	1	5	5	7	4	0
BBDD aplicación	5	4	7	4	0	1	5	4	7	4	0
Contenido audiovisual	5	7	7	3	0	1	5	7	7	3	0
Resultados análisis de tendencias	8	7	7	7	0	1	8	7	7	7	0
Copias de respaldo de la BBDD	9	5	5	5	0	0,1	0,9	0,5	0,5	0,5	0
Ficheros configuración de los sistemas	8	10	5	5	0	1	8	10	5	5	0
Logs de acceso a los sistemas	6	5	5	6	0	1	6	5	5	6	0
Red Local	0	0	7	5	5	1	0	0	7	5	5
Servicio de proveedor de servicios SaaS	0	8	10	8	8	0,1	0	0,8	1	0,8	0,8
Servicio de proveedor de servicios IaaS	0	10	10	10	10	0,1	0	1	1	1	1
Servicio de BBDD como servicio	0	6	10	10	10	0,1	0	0,6	1	1	1
Sistemas de alimentación	0	0,8	0,3	4	3	0,1	0	0,08	0,03	0,4	0,3
CCTV	0	0,2	0,1	1	1	0,1	0	0,02	0,01	0,1	0,1
Equipos de climatización	0	0,2	0,1	1	1	0,1	0	0,02	0,01	0,1	0,1
CEO	4,5	4,5	4,5	9	4,5	0,1	0,45	0,45	0,45	0,9	0,45
Responsable IT	4,5	4	3,5	8	4,5	0,1	0,45	0,4	0,35	0,8	0,45

Tabla 19: Riesgo de los activos tras la ejecución de los proyectos planteados

Responsable de marketing	3,5	3,5	3,5	7	3,5	1	3,5	3,5	3,5	7	3,5
Responsable de ventas	3,5	3,5	3,5	7	3,5	1	3,5	3,5	3,5	7	3,5

Además de contribuir a la mejora del riesgo de la organización, estas medidas mejoran el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC27002, evolucionando hacia un nivel de madurez optimizado.

Tabla 20: Resultados análisis diferencial ISO 27002 tras la ejecución de los proyectos planteados

ISO/IEC 27002 sección	Control ISO 27002	Cumplimiento
5	Políticas de seguridad de la información	60%
6	Organización	34%
7	Seguridad relativa a los RRHH	51%
8	Gestión de activos	36%
9	Control de acceso	56%
10	Criptografía	80%
11	Seguridad física y del entorno	53%
12	Seguridad de las operaciones	55%
13	Seguridad de las comunicaciones	64%
14	Adquisición, desarrollo y mantenimiento de los sistemas	50%
15	Relación con proveedores	60%
16	Gestión de incidentes	46%
17	Continuidad del negocio	87%
18	Cumplimiento	53%

A continuación, se muestra de forma gráfica en un diagrama de radar la evolución de los diferentes dominios y su cumplimiento antes y después de la realización de los diferentes proyectos:

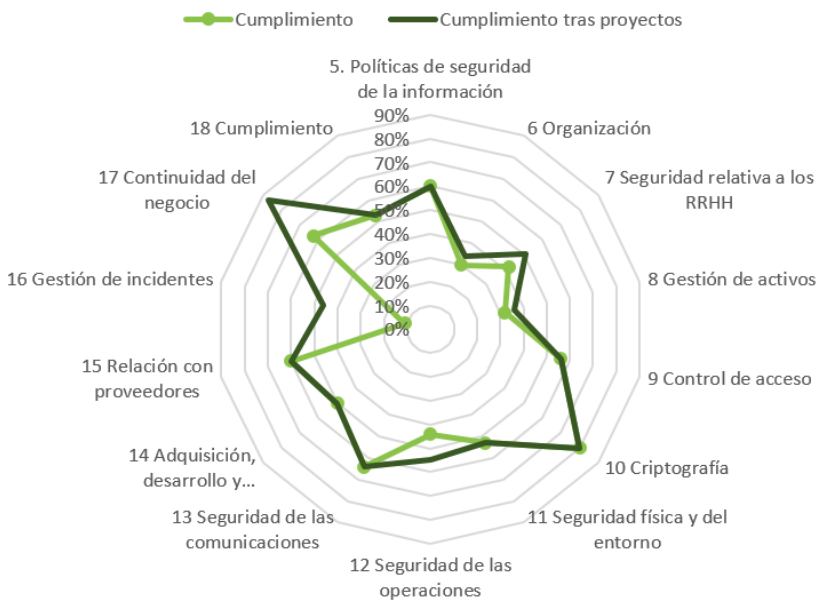


Figura 15: Análisis diferencial tras la ejecución de proyectos

7. Auditoría de cumplimiento

7.1.Introducción

Llegados a esta fase, se tiene conocimiento de los activos de la empresa y las amenazas a las que éstos últimos están expuestos así como su impacto de materialización. En esta etapa se va a evaluar a través de una auditoría hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad, utilizando la ISO/IEC 27002:2013 como marco de control del estado de la seguridad.

7.2.Evaluación de la madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013.

De forma resumida, los dominios analizados son:

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

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

Tabla 21: Grados de madurez según CMM

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN

0 - 9%	**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
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
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más

En el Anexo K, se puede ver una tabla con el nivel de madurez de cada uno de los procesos tras la ejecución de los proyectos y su grado de madurez en función de los niveles del CMM.

A continuación se muestra una tabla resumen con una comparativa de los niveles de madurez de los controles en la Fase inicial y en esta última fase tras la ejecución de los proyectos.

Tabla 22: Comparativa nivel de madurez en fase inicial y fase final

	Control ISO 27002	Nivel de madurez inicial	Nivel de madurez tras proyectos
5.	Políticas de seguridad de la información	60 %	60 %
6	Organización	30 %	34 %
7	Seguridad relativa a los RRHH	42 %	51 %
8	Gestión de activos	32 %	36 %
9	Control de acceso	56 %	56 %
10	Criptografía	80 %	80 %
11	Seguridad física y del entorno	53 %	53 %
12	Seguridad de las operaciones	44 %	55 %
13	Seguridad de las comunicaciones	64 %	64 %
14	Adquisición, desarrollo y mantenimiento de los sistemas	50 %	60 %
15	Relación con proveedores	60 %	60 %
16	Gestión de incidentes	11 %	46 %
17	Continuidad del negocio	63 %	87 %
18	Cumplimiento	53 %	53 %

En referencia a la tabla anterior, y como podemos ver en el gráfico que se muestra a continuación, casi el 51% de los controles han alcanzado un nivel de madurez L2 (reproducible pero intuitivo), y sólo queda un 2% que se quedan con nivel de madurez inexistente.

Además se ha alcanzado un nivel de madurez optimizado en 3 controles.

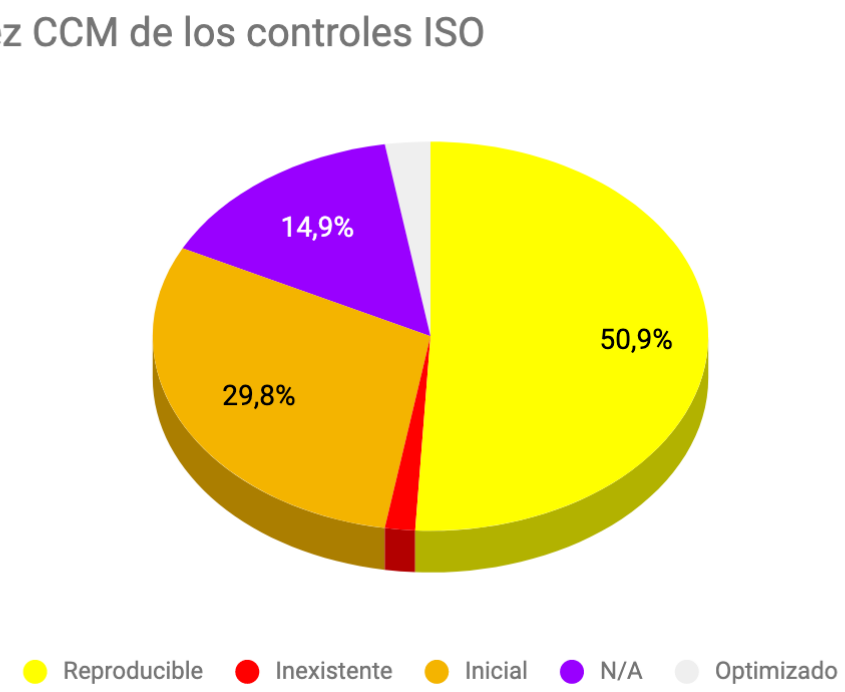


Figura 16: Madurez CCM de los controles ISO 27002

Para la Entidad, el nivel de cumplimiento objetivo es el denominado “Proceso definido”. Esperan llegar a este objetivo, en un plazo de 3 años, una vez que la empresa se estabilice y aumente la plantilla. A continuación, se muestra un gráfico radar comparativo entre el estado actual y el objetivo marcado:

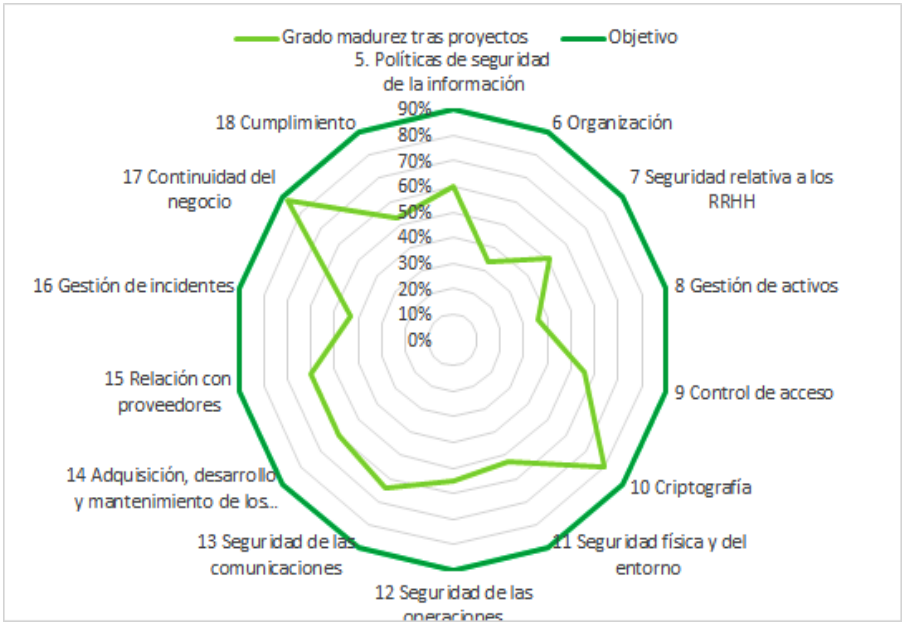


Figura 17: Nivel de madurez actual vs objetivo

De los 114 controles evaluados durante la auditoría llevada a cabo tras la realización de los proyectos, se ha encontrado que hay 9 de ellos que requieren de especial atención debido al hallazgo de 9 No Conformidades, 3 mayores y 6 menores.

Tabla 23: Tabla resumen de No Conformidades

	Control ISO 27002	**No conformidades mayores**	**No conformidades Menores**
5	Políticas de seguridad de la información		
6	Organización	**2**	
7	Seguridad relativa a los RRHH		
8	Gestión de activos	**1**	**2**
9	Control de acceso		
10	Criptografía		
11	Seguridad física y del entorno		**1**
12	Seguridad de las operaciones		**2**
13	Seguridad de las comunicaciones		
14	Adquisición, desarrollo y mantenimiento de los sistemas		
15	Relación con proveedores		
16	Gestión de incidentes		**1**
17	Continuidad del negocio		
18	Cumplimiento		

El siguiente gráfico muestra las no conformidades menores y mayores encontradas según el control de la ISO 27002 al que están asociadas

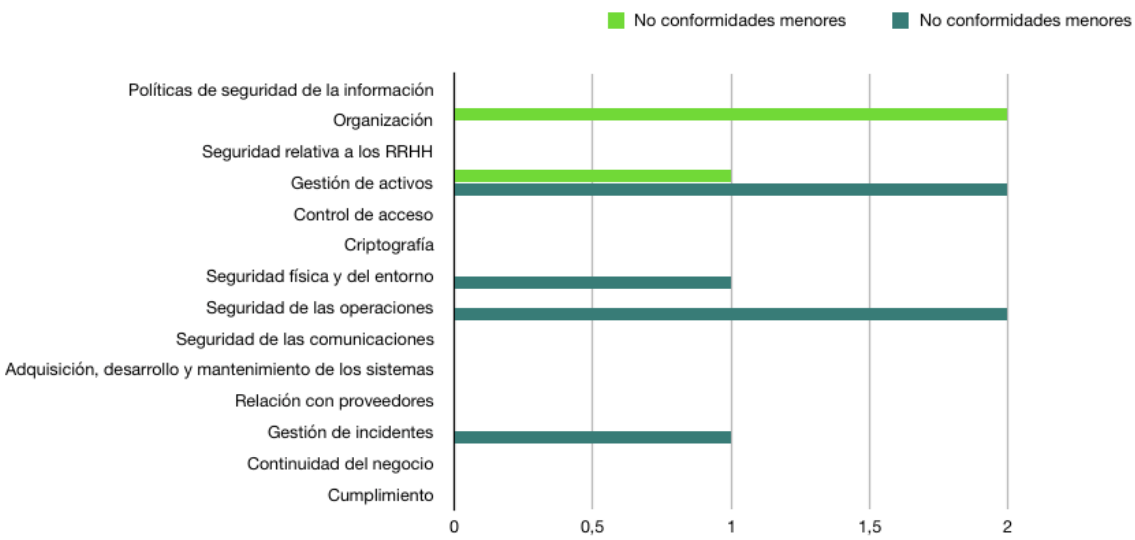


Figura 18: Número de no conformidades por control

El detalle del informe de Auditoría realizado se adjunto en el Anexo L.

8. Conclusiones

Una vez realizadas todas las fases de las que consta el proyecto, se describen las conclusiones extraídas:

- La información es uno de los activos más valiosos y primordiales para TrendTip y una adecuada gestión de sus recursos y activos con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información es fundamental para cualquier empresa.
- La elaboración e implantación del plan director de seguridad ha permitido tener a TrendTip una visión global de los riesgos que pueden afectar la seguridad de los sistemas de información y así establecer controles y medidas efectivas y viables con el propósito de salvaguardar la información y evolucionar hasta el grado de cumplimiento esperado (obsérvese figura).
- De todas las fases que lo constituyen, el análisis de riesgos (Fase 3 del proyecto), constituye la más laboriosa y es donde más ahínco se deben realizar ya que permite identificar el nivel de seguridad en el que se encuentra la organización y los aspectos más débiles para posteriormente poder reforzarlos a través de salvaguardas.
- El apoyo de la dirección es un factor clave para el éxito del proyecto y más en empresas pequeñas como TrendTip donde la inversión en seguridad supone tanto esfuerzo para ella.
- Los objetivos del Plan Director de Seguridad deben encontrarse alineados con los objetivos de negocio de la organización, de modo que la seguridad no lastre el negocio

En términos generales, podemos concluir que TrendTip ha mejorado sustancialmente su nivel de seguridad respecto a la situación inicial planteada. Sin embargo, es importante recalcar que la seguridad es un proceso de mejora continua, y es imprescindible para TrendTip mejorar los procesos que lo constituyen de tal modo que cada vez sean lo más eficientes posibles y consuman los recursos únicamente que demuestren ser imprescindibles dentro de los parámetros de funcionamiento establecidos y asumidos por la Dirección de la organización.

Futuras líneas de trabajo

Como base el trabajo realizado, y como objetivo la mejora continua se propone la realización de otro Plan Director de Seguridad con el objetivo de aumentar el nivel implantación y cumplimiento actualmente obtenido.

Una vez este sistema se encuentre suficientemente maduro, es posible aumentar el alcance, añadiendo más procesos y personas involucradas.

Es posible que debido a que se trata de una startup, los objetivos de negocio cambien y sea necesario adaptar este PDS para que esté conforme con los nuevos procesos de negocio.

Anexo A: Análisis diferencial

Tabla 24: Análisis diferencial ISO 27001

ISO/IEC 27001	Control	Cumplimiento
4	**Contexto de la organización**	**35%**
4.1	Conocimiento de la organización y su contexto	**20%**
4.2	Compresión de las necesidades y expectativas de las partes interesadas	**40%**
4.3	Determinación del alcance del sistema de gestión de seguridad de la información	**60%**
4.4	Sistema de gestión de seguridad de la información	**20%**
5	**Liderazgo**	**67%**
5.1	Liderazgo y compromiso	**60%**
5.2	Política	**80%**
5.3	Roles, responsabilidades y autoridades en la organización	**60%**
6	**Planificación**	**70%**
6.1	Acciones para tratar riesgos y oportunidades	**60%**
6.2	Objetivos de seguridad de la información	**80%**
7	**Soporte**	**28%**
7.1	Recursos	**20%**
7.2	Competencia	**20%**
7.3	Toma de conciencia	**40%**
7.4	Comunicación	**20%**
7.5	Información documentada	**40%**
8	**Operación**	**7%**
8.1	Planificación y control operacional	**0%**
8.2	Evaluación de riesgos de seguridad de la información	**0%**
8.3	Tratamiento de riesgos de seguridad de la información	**20%**
9	**Evaluación del desempeño**	**13%**
9.1	Seguimiento, medición, análisis y evaluación	**20%**
9.2	Auditoría interna	**20%**
9.3	Revisión por la dirección	**0%**
10	**Mejora**	**20%**
10.1	No conformidades y acciones correctivas	**40%**
10.2	Mejora continua	**0%**

Tabla 25: Análisis diferencial ISO 27002

ISO/IEC 27002	Control	Cumplimiento	
5	**Políticas de seguridad de la información**	**60%**	**Bien definido**
5.1	Directrices de gestión de seguridad de la información	60%	Bien definido
5.1.1	Políticas para la seguridad de la información	60%	Bien definido
5.1.2	Revisión de las políticas de seguridad de la información	60%	Bien definido
6	**Organización de la seguridad de la información**	**30%**	**Realizado informalmente**
6.1	Organización interna	20%	Realizado informalmente
6.1.1	Roles y responsabilidades en seguridad de la información	60%	Bien definido
6.1.2	Segregación de tareas	20%	Realizado informalmente
6.1.3	Contacto con las autoridades	0%	No realizado
6.1.4	Contacto con grupos de interés especial	0%	No realizado
6.1.5	Seguridad de la información en la gestión de proyectos	20%	Realizado informalmente
6.2	Los dispositivos móviles y el teletrabajo	40%	Planificado
6.2.1	Política de dispositivos móviles	40%	Planificado
6.2.2	Teletrabajo		N/A
7	**Seguridad relativa a los recursos humanos**	**42%**	**Planificado**
7.1	Antes del empleo	60%	Bien definido
7.1.1	Investigación de antecedentes	60%	Bien definido
7.1.2	Términos y condiciones del empleo	60%	Bien definido
7.2	Durante el empleo	27%	Realizado informalmente
7.2.1	Responsabilidades de gestión	20%	Realizado informalmente

Tabla 25: Análisis diferencial ISO 27002

7.2.2	Concienciación, educación y capacitación en seguridad de la información	20%	Planificado
7.2.3	Proceso disciplinario	40%	Planificado
7.3	Finalización del empleo o cambio en el puesto de trabajo	40%	Planificado
7.3.1	Responsabilidades ante la finalización o cambio	**40%**	Planificado
8	**Gestión de activos**	**32 %**	**Planificado**
8.1	Responsabilidad sobre los activos	30 %	Realizado informalmente
8.1.1	Inventario de activos	40 %	Planificado
8.1.2	Propiedad de los activos	40 %	Planificado
8.1.3	Uso aceptable de los activos	20 %	Realizado informalmente
8.1.4	Devolución de activos	20 %	Realizado informalmente
8.2	Clasificación de la información	40 %	Planificado
8.2.1	Clasificación de la información	40 %	Planificado
8.2.2	Etiquetado de la información	40 %	Planificado
8.2.3	Manipulado de la información	40 %	Planificado
8.3	Manipulación de los soportes	27 %	Realizado informalmente
8.3.1	Gestión de soportes extraíbles	20 %	Realizado informalmente
8.3.2	Eliminación de soportes	20 %	No realizado
8.3.3	Soportes físicos en tránsito	40 %	Planificado
9	**Control de acceso**	**44%**	**Planificado**
9.1	Requisitos de negocio para el control de acceso	50%	Planificado
9.1.1	Política de control de acceso	40%	Planificado
9.1.2	Acceso a las redes y a los servicios de red	60%	Bien definido
9.2	Gestión de acceso de usuario	60%	Cuantitativamente controlado
9.2.1	Registro y baja de usuario	60%	Bien definido

Tabla 25: Análisis diferencial ISO 27002

9.2.2	Provisión de acceso de usuario	60%	Bien definido
9.2.3	Gestión de privilegios de acceso	60%	Bien definido
9.2.4	Gestión de la información secreta de autenticación de usuarios	60%	Bien definido
9.2.5	Revisión de los derechos de acceso de usuario	60%	Bien definido
9.2.6	Retirada o reasignación de los derechos de acceso	60%	Bien definido
9.3	Responsabilidades del usuario	60%	Bien definido
9.3.1	Uso de la información secreta de autenticación	**60%**	Bien definido
9.4	Control de acceso a sistemas y aplicaciones	52%	Bien definido
9.4.1	Restricción del acceso a la información	60%	Bien definido
9.4.2	Procedimientos seguros de inicio de sesión	60%	Bien definido
9.4.3	Sistema de gestión de contraseñas	60%	Bien definido
9.4.4	Uso de utilidades con privilegios del sistema	40%	Planificado
9.4.5	Control de acceso al código fuente de los programas	40%	Planificado
10	**Criptografía**	**80%**	**Cuantitativamente controlado**
10.1	Controles criptográficos	80%	Cuantitativamente controlado
10.1.1	Política de uso de controles criptográficos	80%	Cuantitativamente controlado
10.1.2	Gestión de claves	80%	Cuantitativamente controlado
11	**Seguridad física y del entorno**	**53%**	**Planificado**
11.1	Áreas seguras	60%	Bien definido
11.1.1	Perímetro de seguridad física	N/A	
11.1.2	Controles físicos de entrada	N/A	
11.1.3	Seguridad de oficinas, despachos y recursos	60%	Bien definido

Tabla 25: Análisis diferencial ISO 27002

11.1.4	Protección contra amenazas externas y ambientales	60%	Bien definido
11.1.5	El trabajo en áreas seguras	N/A	
11.1.6	Áreas de carga y descarga	N/A	
11.2	Seguridad de los equipos	46%	Planificado
11.2.1	Emplazamiento y protección de equipos	40%	Planificado
11.2.2	Instalaciones de suministro	N/A	
11.2.3	Seguridad del cableado	N/A	
11.2.4	Mantenimiento de los equipos	40%	Planificado
11.2.5	Retirada de materiales propiedad de la empresa	40%	Planificado
11.2.6	Seguridad de los equipos fuera de las instalaciones	40%	Planificado
11.2.7	Reutilización o eliminación segura de equipos	60%	Bien definido
11.2.8	Equipo de usuario desatendido	60%	Bien definido
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	40%	Planificado
12	**Seguridad de las operaciones**	**44%**	**Planificado**
12.1	Procedimientos y responsabilidades operacionales	27%	Realizado informalmente
12.1.1	Documentación de procedimientos de operación	40%	Planificado
12.1.2	Gestión de cambios	20%	Realizado informalmente
12.1.3	Gestión de capacidades	20%	Realizado informalmente
12.1.4	Separación de los recursos de desarrollo, prueba y operación	N/A	
12.2	Protección contra el software malicioso	60%	Bien definido
12.2.1	Controles contra el código malicioso	60%	Bien definido
12.3	Copias de seguridad	60%	Bien definido
12.3.1	Copias de seguridad de la información	**60%**	Bien definido

Tabla 25: Análisis diferencial ISO 27002

12.4	Registros y supervisón	0%	No realizado
12.4.1	Registro de eventos	0%	No realizado
12.4.2	Protección de la información de registro	0%	No realizado
12.4.3	Registro de administración y operación	0%	No realizado
12.4.4	Sincronización del reloj	0%	No realizado
12.5	Control del software en explotación	60%	Bien definido
12.5.1	Instalación de software en explotación	60%	Bien definido
12.6	Gestión de la vulnerabilidad técnica	40%	Planificado
12.6.1	Gestión de vulnerabilidades técnicas	40%	Planificado
12.6.2	Restricción en la instalación de software	40%	Planificado
12.7	Consideraciones sobre la auditoría de sistemas de información	60%	Bien definido
12.7.1	Controles de auditoría de sistemas de información	60%	Bien definido
13	**Seguridad de las comunicaciones**	**64%**	**Bien definido**
13.1	Gestión de la seguridad de las redes	73%	Bien definido
13.1.1	Controles de red	60%	Bien definido
13.1.2	Seguridad de los servicios de red	60%	Bien definido
13.1.3	Segregación de redes	100 %	Mejora continua
13.2	Intercambio de información	55%	Planificado
13.2.1	Políticas y procedimientos de intercambio de información	60%	Bien definido
13.2.2	Acuerdos de intercambio de información	60%	Bien definido
13.2.3	Mensajería electrónica	60%	Bien definido
13.2.4	Acuerdos de confidencialidad o no revelación	40%	Planificado
14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**50%**	**Planificado**

Tabla 25: Análisis diferencial ISO 27002

14.1	Requisitos de seguridad en sistemas de información	60%	Bien definido
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	60%	Bien definido
14.1.2	Asegurar a los servicios de aplicaciones en redes públicas	60%	Bien definido
14.1.3	Protección de las transacciones de servicios de aplicaciones	60%	Bien definido
14.2	Seguridad en el desarrollo y en los procesos de soporte	40,00%	Planificado
14.2.1	Política de desarrollo seguro	N/A	
14.2.2	Procedimiento de control de cambios en sistemas	N/A	
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	N/A	
14.2.4	Restricciones a los cambios en los paquetes de software	40%	Planificado
14.2.5	Principios de ingeniería de sistemas seguros	N/A	
14.2.6	Entorno de desarrollo seguro	N/A	
14.2.7	Externalización del desarrollo de software	40%	Planificado
14.2.8	Pruebas funcionales de seguridad de sistemas	N/A	
14.2.9	Pruebas de aceptación de sistemas	N/A	
14.3	Datos de prueba	N/A	
14.3.1	Protección de los datos de prueba	**N/A**	
15	**Relación con proveedores**	**60%**	**Bien definido**
15.1	Seguridad en las relaciones con los proveedores	60%	Bien definido
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	60%	Bien definido
15.1.2	Requisitos de seguridad en contratos con terceros	60%	Bien definido
15.1.3	Cadena de suministros de tecnología de la información y de las comunicaciones	60%	Bien definido

Tabla 25: Análisis diferencial ISO 27002

15.2	Gestión de la provisión de servicios del proveedor	60%	Bien definido
15.2.1	Control y revisión de la provisión de servicios del proveedor	60%	Bien definido
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	60%	Bien definido
16	**Gestión de incidentes de seguridad de la información**	**11%**	**No realizado**
16.1	Gestión de incidentes de seguridad de la información y mejoras	11%	No realizado
16.1.1	Responsabilidades y procedimientos	20%	Realizado informalmente
16.1.2	Notificación de los eventos de seguridad de la información	20%	Realizado informalmente
16.1.3	Notificación de puntos débiles de la seguridad	0%	No realizado
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	20%	Realizado informalmente
16.1.5	Respuesta a incidentes de seguridad de la información	20%	Realizado informalmente
16.1.6	Aprendizaje de los incidentes de seguridad de la información	0%	No realizado
16.1.7	Recopilación de evidencias	0%	No realizado
17	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**	**63%**	**Bien definido**
17.1	Continuidad de la seguridad de la información	27%	Cuantitativamente controlado
17.1.1	Planificación de la continuidad de la seguridad de la información	40%	Planificado
17.1.2	Implementar la continuidad de la seguridad de la información	40%	Planificado
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0%	No realizados
17.2	Redundancias	100 %	Mejora continua
17.2.1	Disponibilidad de los recursos de tratamiento de la información	100 %	Mejora continua

Tabla 25: Análisis diferencial ISO 27002

18	**Cumplimiento**	**53%**	**Planificado**
18.1	Cumplimiento de los requisitos legales y contractuales	60%	Bien definido
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	60%	Bien definido
18.1.2	Derechos de propiedad intelectual	60%	Bien definido
18.1.3	Protección de los registros de la organización	60%	Bien definido
18.1.4	Protección y privacidad de la información de carácter personal	60%	Bien definido
18.1.5	Regulación de los controles criptográficos	60%	Bien definido
18.2	Revisiones de la seguridad de la información	47%	Planificado
18.2.1	Revisión independiente de la seguridad de la información	60%	Bien definido
18.2.2	Cumplimiento de las políticas y normas de seguridad	20%	Realizado informalmente
18.2.3	Comprobación del cumplimiento técnico	60%	Bien definido

Anexo B: Política y marco normativo de seguridad de la información

B.1- Política de seguridad de la información

Objetivo: Establecer las medidas aplicables en TrendTip para preservar la confidencialidad, disponibilidad e integridad de la información bajo responsabilidad de los empleados de la empresa.

Alcance: Empleados y CEO de la empresa TrendTip

Política General:

Los empleados y el CEO deben:

1. Emplear las herramientas (hardware, software y servicios) tecnológicas, proporcionadas por TrendTip para el desempeño de las funciones que le son encomendadas.
2. Utilizar la información que TrendTip pone a su disposición exclusivamente para el desempeño de sus funciones. Protegiéndola y preservándola de aquellos usos inadecuados, que pudieran provocar perjuicios económicos o deterioro de la reputación de la empresa y sus clientes. Identificando el tipo y nivel que corresponda establecido en la normativa de "Clasificación de información".
3. Preservar el principio de confidencialidad por medio de:
    a. Utilizar las credenciales de acceso lógico (usuario y contraseña) en calidad de personales e intransferibles.
    b. Bloquear la sesión de trabajo en los ordenadores portátiles, cuando no se estén utilizando.
    c. Evitar accesos no autorizados a la información en formato físico utilizando políticas de escritorio limpio.
4. Preservar el principio de integridad a través de:
    a. Asegurarse de que se cuenta con los privilegios mínimos necesarios para la ejecución de sus actividades.
    b. Gestionar el acceso a información, bajo responsabilidad o control de otros departamentos, únicamente por los canales autorizados.
5. Preservar el principio de disponibilidad a través del:
    a. Uso seguro de las herramientas tecnológicas, las cuales deben ser instaladas, configuradas, reparadas o desinstaladas únicamente por el responsable IT.
    b. Empleo de software estrictamente institucional, autorizado para su puesto y funciones.
    c. Uso de las redes de datos, en apego a lo establecido en la normativa "Acceso seguro a las redes".

En caso de presentarse situaciones que pongan en riesgo los servicios internos, a sus clientes o terceros que sean reconocidas como “ciberataques”, se deberán aplicar las medidas y planes de actuación definidos en el procedimiento de gestión de incidentes.

En caso de detectar o confirmar situaciones de incumplimiento de la presente política se podrá las acciones administrativas o legales que competan.

B2 - Norma de gestión de activos

A lo largo de esta norma se proveen las directrices a seguir para la implementación de medidas de seguridad sobre los Sistemas de Información basados en la clasificación de la información que manejan, y adecuados a la valoración del riesgo a los que están expuestos. La norma definirá todas las directrices en relación a:

- **Clasificación de la Información**: La información podrá ser clasificada, según el modelo de clasificación de la información, en los siguientes niveles:
    - Información pública: Es la información que puede ser divulgada o publicada en los canales digitales o en formato papel. La información pública no dispone de limitaciones de acceso
    - Información confidencial: Es la información necesaria para el correcto desempeño de las funciones dentro de la Entidad y cuya divulgación intencionada o accidental podría suponer un impacto económico. Este tipo de información es accesible únicamente por listas cerradas de personas (p.ej. informes de auditoría, informes de estrategia corporativa, etc.).
    - Información secreta: Es la información conocida únicamente por el propietario de la misma (p.ej. contraseñas, claves criptográficas, etc.).
- **Información sujeta a regulación**: Es la información que está sujeta a cumplimiento legal, regulatorio o contractual. Se deberán incorporar los controles específicos y deberá recibir el tratamiento necesario para cumplir con los requerimientos establecidos.
- **Uso correcto de activos:** Los empleados deben utilizar los activos utilizándolos de forma adecuada para lo que se han proporcionado, y manteniendo la confidencialidad de la información de acuerdo a su clasificación.
- **Gestión de medios extraíbles y destrucción de medios físicos:** No se autoriza el uso de medios extraíbles para la transmisión de información de la Entidad. Se realizará una destrucción adecuada de los activos que hayan contenido información de la empresa, de tal forma que permita asegurar la no recuperación de la misma. En el caso de activos de información que contengan datos en formato digital, se asegurará que los datos no puedan ser recuperados y que el dispositivo que los almacenaba no pueda ser reutilizado.
- **Transferencia por medios físicos:** La información que sea transferida entre sistemas ha de mantener los niveles de seguridad establecidos en función de su clasificación.

B3- Norma de gestión de las operaciones

La gestión de los sistemas y aplicaciones debe asegurar que un usuario sea capaz de realizar toda función necesaria para el correcto desempeño de su trabajo con los mínimos privilegios de acceso. Además, debe asegurar la correcta segregación de funciones de acuerdo con los roles y responsabilidades de cada usuario. Esta Norma provee, para los activos de información, las directrices a seguir en el mantenimiento de la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida. Para ello se desarrollan las medidas de seguridad a contemplar en:

- **Gestión de código malicioso.** Las estaciones de trabajo y los servidores propiedad de TrendTip que lo permitan, deben contar con medidas de seguridad contra código malicioso, tales como virus, gusanos, troyanos o malware similar, de forma que los protejan contra los diversos daños que estos ataques puedan causar. El responsable de seguridad es responsable de verificar el estado de las medidas relacionadas con el malware y de realizar una revisión de los sistemas, la implementación de medidas y el uso del software especializado para la detección y contención de los eventos relacionados con código malicioso. En el caso de detectar una amenaza, se habilitarán las medidas necesarias para realizar una contención efectiva, incluyendo la desconexión si se considera oportuno.
- **Gestión de copias de respaldo**. La información almacenada en las copias de respaldo, tanto software como datos, debe mantener las mismas medidas de seguridad que tenían en los Sistemas de Información origen. Se habilitarán controles para asegurar la integridad de los datos almacenados en copias de respaldo. El acceso a las copias de respaldo está restringido mediante control físico, lógico, o cifrado de la Información.
- **La destrucción de medios utilizados** para el almacenamiento de copias de respaldo se registrará adecuadamente y deberá ser comunicada al área de seguridad.

B4 - Norma de Gestión de la continuidad de negocio.

La Continuidad de Negocio es una disciplina de gerencia empresarial que tiene como misión preparar a las organizaciones para mantener su actividad crítica , en unos mínimos previamente establecidos, ante cualquier situación que, siendo muy poco frecuente, provoque una disrupción operacional grave en su normal funcionamiento.

Esta Norma provee una serie de medidas preventivas, que deben estar integrados como un factor más en la gestión empresarial, y reactivas, a través de planes específicos, llamados Planes de Continuidad (PC's), que agrupan la gestión de la crisis y el Plan de Recuperación (PR). Ambas actuaciones requieren de un marco de gobierno que permita su inclusión en los esquemas organizativos de las entidades, de tal manera que no constituyan actividades esporádicas e improvisadas ante estas contingencias graves imprevistas.

Plan de continuidad:

Los objetivos del plan de continuidad son:

- Gestionar situaciones de Crisis: Establecer de forma documental las responsabilidades, mecanismos de comunicación, valoración y decisión, y procedimientos de actuación en situaciones excepcionales de crisis en el ámbito del PC.
- Establecer Planes de Recuperación: Desarrollar planes de recuperación de las actividades consideradas críticas, ante una situación que impida o imposibilite la continuidad de las mismas, durante un periodo determinado de tiempo. Dichos Planes de Recuperación abordan los siguientes escenarios:
    - Escenario Indisponibilidad del Centro
    - Escenario Indisponibilidad de RRHH críticos
    - Escenario Indisponibilidad de un proveedor crítico

B5 - Norma de gestión de incidentes

La gestión de los sistemas y aplicaciones debe asegurar que todas las actividades realizadas quedan registradas y monitorizadas. Para el desarrollo de esta norma se ha considerado como incidente cualquier alteración de la operativa diaria que pueda producir un perjuicio en los Sistemas de Información de la Entidad. En esta consideración quedarían englobados tanto eventos como incidentes, incidencias y vulnerabilidades.

El objetivo principal de la Norma es el de ser un marco de referencia ante incidentes, eventos y vulnerabilidades, disminuyendo así el riesgo asociado, para permitir la continuidad de las operaciones. Para ello se desarrollan los siguientes aspectos:

- **Gestión de incidentes:** directrices para la gestión de incidentes mediante un Plan de Respuesta. En él se establecen las directrices para documentar, monitorear, analizar, mitigar y reportar cualquier tipo de incidente físico o lógico de Seguridad de la Información. Adicionalmente asegura que los incidentes son gestionados y reportados adecuadamente.
- **Gestión de vulnerabilidades:** Se deben realizar revisiones periódicas de los sistemas de información y los dispositivos de red, para la detección, notificación y posterior remediación o mitigación de vulnerabilidades. El responsable de seguridad debe velar por la resolución de las vulnerabilidades detectadas en los sistemas de información. Los Sistemas de Información de la Entidad son revisados y auditados periódicamente para buscar nuevas vulnerabilidades y verificar la resolución de las detectadas previamente. Se deben clasificar las vulnerabilidades en diferentes niveles de criticidad atendiendo entre otros a los criterios de severidad, alcance de la detección y grado de exposición del activo. En función de esta clasificación, se aplican los procedimientos pertinentes de resolución y mitigación.
- **Lecciones aprendidas:** se tienen mecanismos para la mejora de los planes de recuperación y contención en función de eventos pasados. deberán proponer mejoras en las medidas de seguridad para evitar la probabilidad o repetición de incidentes conocidos. Además, se deberá mejorar la concienciación de los empleados basándose en la información obtenido de los incidentes de seguridad.

B6 - Norma de gestión de servicios cloud

El presente documento enuncia las directrices generales de Seguridad de la Información con el fin de conseguir una adecuada protección de dicha información en los entornos Cloud y actuar de conformidad con lo exigido por los organismos reguladores, abordando los siguientes puntos:

- Consideraciones previas a la contratación del servicio y relación con el proveedor.
- Requerimientos de Seguridad de la Información en entornos Cloud.
- Control de acceso

Consideraciones previas a la contratación del servicio

Previo a la contratación de cualquier servicio cloud, que suponga un cambio importante en la infraestructura de la organización, se deben realizar los siguientes pasos:

- Solicitar al proveedor de servicios toda la información correspondiente a sus controles y medidas de seguridad. El responsable debe comprobar que estos se hallan alineados con los requerimientos de seguridad de la Entidad.
- Evaluar y determinar el riesgo de externalización del servicio en el proveedor Cloud prestando especial atención a la legislación vigente.
- En caso de contratación, verificar que las cláusulas firmadas incluyen la notificación a la Entidad sobre los cambios de las medidas de seguridad y cumplimiento normativo que puedan producirse. En caso de producirse dichos cambios, deberá llevarse a cabo una nueva evaluación de la iniciativa Cloud y reevaluar las medidas de seguridad si procede

Requerimientos de Seguridad

La infraestructura que alberga los servicios de Cloud deberá contar con las medidas de Seguridad requeridas al inicio de la contratación. Los servicios Cloud deben tener la capacidad de generar registros de actividad para poder ser revisados por parte de la Entidad.

Control de Acceso

El acceso a los datos alojados en la infraestructura Cloud será gestionado en base al principio del mínimo privilegio y de segregación de funciones. Los accesos a la infraestructura Cloud deben ser monitorizados. Deberán ser definidos diferentes perfiles de acceso a la infraestructura y a la información en función de las tareas asignadas en el servicio externalizado. Deben estar específicamente identificados los usuarios que tienen acceso a las cuentas con mayor nivel de privilegios.

B7 - Norma de gestión de cumplimiento

Todo el personal que colabore con TrendTip debe cumplir la Política de Seguridad de la Información definida por la Entidad, así como la legislación y la normativa vigente y los requerimientos contractuales adheridos por parte de la Entidad. El cumplimiento con los requerimientos que se derivan de terceros ajenos a la Entidad resulta de vital importancia

para generar confianza en las operaciones y para responder adecuadamente ante reguladores y legisladores.

Esta norma describe los ámbitos de:

Cumplimiento legal, regulatorio y contractual: define los criterios generales a seguir dentro de la Entidad para evitar incumplimientos de carácter legal, regulatorio y contractual relacionados con la Seguridad de la Información.

Cumplimiento Legal, Regulatorio y Contractual

Derechos de Propiedad Intelectual Los empleados deberán utilizar el software facilitado por TrendTip para el desempeño de sus funciones y evitar el uso de software no licenciado.

Protección de Registros Los registros de actividad generados por los Sistemas de Información deben estar protegidos cumpliendo con los requerimientos de carácter legal, regulatorio y contractual a los que estén sujetos. Los registros de actividad deben tener un período de retención en función de la legislación o regulación que les sea aplicable.

Protección de Datos y Privacidad: TredTip debe cumplir con la regulación específica de privacidad de la información, tanto para información de clientes como del personal de la Entidad, siendo el área de seguridad la que propondrá las medidas tecnológicas específicas de seguridad para su cumplimiento

Anexo C: Procedimiento de auditorías internas

Objetivo:

Para vigilar el adecuado funcionamiento del sistema de gestión de seguridad de la información, contribuir a la mejora de la efectividad de los controles internos y comprobar también el cumplimiento de los posibles requisitos legales en materia de seguridad de la información, la dirección de la empresa ha establecido la necesidad de realizar una auditoría del SGSI con carácter anual o cada vez que haya un cambio significativo del perfil de riesgo tecnológico.

Alcance:

El alcance de la auditoría interna será el SGSI completo de acuerdo a los requisitos de la norma ISO/IEC 27001:2013.

Roles y responsabilidades:

Esta auditoría se llevará a cabo por una empresa externa debido al escaso personal con el que cuenta TrendTip. Para asegurarse que la empresa proveedora del servicio cuenta con profesionales adecuados para el desarrollo de su tarea, se exigirá el CV de los auditores que vayan a realizar dicha auditoría. Estos auditores deben cumplir con los requisitos establecidos en la norma ISO 19011 en cuanto a: integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y un enfoque basado en la evidencia.

Por parte de TrendTip, se designará un responsable de la auditoría que será el encargado de acompañar al auditor en todo momento durante la realización de ésta y proporcionarle las evidencias que solicite.

Una vez finalizada la auditoría, será el responsable de la auditoría quien exponga a la dirección las posibles acciones correctivas para que la dirección las apruebe o rechace.

Metodología:

La metodología a utilizar durante la auditoría será la descrita en la norma ISO 19011 de “Directrices de para la auditoría de sistemas de gestión”:

1. Realización de una reunión de apertura donde se confirme el plan de auditoría
2. Revisión de la documentación del sistema de gestión.
3. Recopilación y verificación de la información a través de un muestreo aleatorio.
4. Redacción de los hallazgos de auditoría.
5. Elaboración de las conclusiones de auditoría.
6. Realización de la reunión de cierre donde se detallarán a la dirección los hallazgos encontrados (No conformidades, Observaciones y puntos de mejora).
7. Redacción del informe final de auditoría. Este último debe proporcionar un registro preciso, conciso y claro de la auditoría y debe incluir los siguientes puntos:
    - Fecha y lugares donde se ha realizado la auditoría

- Objetivo de la auditoría, alcance y criterios.
- Equipo de auditoría y participantes de TrendTip.
- Hallazgos y evidencias de auditoría.
- Conclusiones.
- Declaración de los criterios que se han cumplido.

Calendario previsto:

En el diagrama de Gantt que se muestra a continuación se detalla el calendario de auditorías previsto para TrendTip para los 3 próximos años. En cada auditoría se evaluarán los 114 controles del Anexo A de la ISO 27001 que aplican según la SOA (Declaración de aplicabilidad) definida.

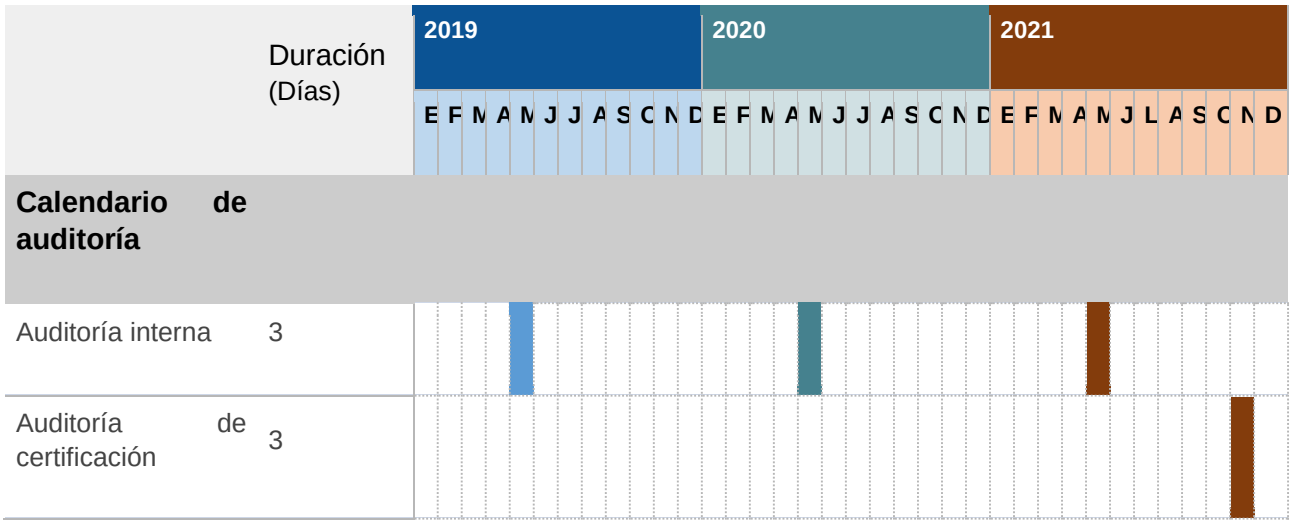


Figura 19 : Diagrama de Gantt de auditorías

Anexo D: Gestión de indicadores

Tabla 26: Tabla de indicadores

	Control	Indicador	Descripción	Objetivo
5	**Políticas de seguridad de la información**			
5.1	Directrices de gestión de seguridad de la información	IDC1	(Políticas aprobadas/Políticas totales)*100	80%
		IDC2	(Políticas actualizadas y revisadas/Políticas totales)*100	80%
6	**Organización de la seguridad de la información**			
6.1	Organización interna	IDC3	Empleados que han recibido y aceptado formalmente sus roles y responsabilidades en materia de seguridad/Número total de empleados	100%
7	**Seguridad relativa a los recursos humanos**			
7.1	Antes del empleo	IDC4	Número de empleados contratados para los que se han comprobado los antecedentes/Número total de empleados contratados	70%
7.2	Durante el empleo	IDC5	Número de casos phising detectados por los empleados	
8	**Gestión de activos**			
8.1	Responsabilidad sobre los activos	IDC6	Porcentaje de activos con responsables definidos	95%
8.2	Clasificación de la información	IDC7	Porcentaje de activos de información en cada categoría de clasificación	80%

Tabla 26: Tabla de indicadores

8.3	Manipulación de los soportes	IDC8	Porcentaje de soportes de backup o archivo que están cifrados	100%
9	**Control de acceso**			
9.1	Requisitos de negocio para el control de acceso	IDC9	Política de acceso a la información actualizada	1 vez al año
9.2	Gestión de acceso de usuario	IDC10	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos	1hora
9.3	Responsabilidades del usuario	IDC11	Porcentaje de contraseñas de usuario almacenadas en sistemas no seguros	0%
9.4	Control de acceso a sistemas y aplicaciones	IDC12	Porcentaje de sistemas con backup que están totalmente cifrados	100%
10	**Criptografía**			
10.1	Controles criptográficos	IDC13	Porcentaje de sistemas con información sensible cifrados	95%
11	**Seguridad física y del entorno**			
11.1	Áreas seguras	IDC14	Porcentaje de personas no autorizadas que han accedido a zonas seguras	0%
11.2	Seguridad de los equipos	IDC15	Número de incidentes en los equipos del personal interno	2 incidentes
12	**Seguridad de las operaciones**			
12.1	Procedimientos y responsabilidades operacionales	IDC16		
12.2	Protección contra el software malicioso	IDC17	Porcentaje de incidentes por malware gestionados	100%

Tabla 26: Tabla de indicadores

12.3	Copias de seguridad	IDC18	Porcentaje de sistemas con datos críticos con copia de seguridad realizada en el último mes	100%
12.4	Registros y supervisión	IDC19	Porcentaje de sistemas con datos críticos monitorizados	100%
12.5	Control del software en explotación	IDC20	Porcentaje de intentos de instalación de licencias ilegales de Software	0%
12,6	Gestión de la vulnerabilidad técnica	IDC21	Número de vulnerabilidades Críticas abiertas	0 críticas
		IDC22	Porcentaje de vulnerabilidades Críticas resueltas	100%
12.7	Consideraciones sobre la auditoría de sistemas de información	IDC23	Porcentaje de no conformidades y puntos de mejora encontradas en las auditorías gestionadas y solucionadas	100%
13	**Seguridad de las comunicaciones**			
13.1	Gestión de la seguridad de las redes	IDC24	Número de incidentes de seguridad de red identificados/Número de incidentes de seguridad de red resueltos	100%
13.2	Intercambio de información	IDC25		
15	**Relación con proveedores**			
15.1	Seguridad en las relaciones con los proveedores	IDC26	Porcentaje de contratos con los proveedores con cláusulas relativas a seguridad de la información en cuanto a confidencialidad de los datos utilizados	90%
15.2	Gestión de la provisión de servicios del proveedor	IDC27	Porcentaje de SLAs incumplidos	80%
16	**Gestión de incidentes de seguridad de la información**			

Tabla 26: Tabla de indicadores

16.1	Gestión de incidentes de seguridad de la información y mejoras	IDC28	Tiempo medio de resolución de los incidentes	Para incidentes críticos < 2 horas
		IDC29	% de incidentes críticos gestionados y resueltos	80%
17	**Aspectos de segruidad de la información para la gestión de la continuidad del negocio**			
17.1	Continuidad de la seguridad de la información	IDC30	% del total de sistemas de alto y medio impacto en los que se ha probado los RTO y RPO correspondientes en restauración.	100%
18	**Cumplimiento**			
18.1	Cumplimiento de los requisitos legales y contractuales	IDC31	Número de requisitos legales analizados y clasificados por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).	100%
18.2	Revisiones de la seguridad de la información	IDC32	Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos	100%

Tabla 9: Tabla de indicadores

Anexo E: Procedimiento de revisión por la dirección

La Dirección declara que la información es uno de los recursos más importantes de la empresa, por lo que considera su protección y la de los activos que la sustentan un compromiso fundamental. Para conseguirlo, a Dirección de TrendTip debe reunirse para revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información.

- Esta revisión debe incluir consideraciones sobre:
- El estado de las acciones con relación a las revisiones previas por la dirección.
- Los cambios en las cuestiones externas e internas que sean pertinentes al Sistema de Gestión de Seguridad de la Información.
- Retroalimentación sobre el desempeño de la seguridad de la información
- Retroalimentación de las partes interesadas.
- Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos
- Las oportunidades de mejora continua.
- Desarrollo de una política de seguridad de la información.
- Garantizar el cumplimiento de planes y objetivos de Sistema de Gestión de Seguridad de la Información.
- Constituir roles y responsabilidades de seguridad de la información.
- Informar a la empresa la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad.
- Designar todos los recursos necesarios para llevar a cabo el SGSI.
- Determinar todos los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asignar los recursos suficientes para todas las fases del SGSI.
- Garantizar que se realizan todas las auditorías internas.
- Llevar a cabo revisiones periódicas del SGSI.

Anexo F: Gestión roles y responsabilidades

A lo largo de este documento se definen los roles y responsabilidades que intervienen en el Sistema de Gestión de Seguridad de la información:

- CISO (Chief Information Security Office).
- Comité de seguridad.

CISO (Chief Information Security Office)

TrendTip define la figura de CISO, como el máximo responsable del área de Seguridad de la Información en todos sus ámbitos, incluyendo la Ciberseguridad y la gestión del Riesgo. Este rol será desempeñado por el responsable de TI de la organización.

El CISO debe gestionar la Seguridad de la entidad teniendo en cuenta cuestiones tales como:

- la evaluación de riesgos,
- la gestión de riesgos, las decisiones de control,
- los acuerdos con proveedores de servicios,
- la gestión de las vulnerabilidades,
- gestión de los incidentes de seguridad y
- elaboración y prueba de los planes de recuperación y de continuidad de negocio.

Comité de seguridad

El Comité de seguridad está coordinado por el CISO, y participará también el CEO de la empresa. Sus objetivos son:

- Gestionar el riesgo tecnológico y la ciberseguridad de la empresa
- Coordinar el ámbito de la seguridad mediante: la definición de políticas, establecimiento de arquitecturas, procesos de implantación, controles de operación, monitorización de sistemas, verificaciones técnicas y el cumplimiento de las políticas, normas, procedimientos, guías, planes y estándares,
- Establecer responsabilidades en materia de Seguridad de la información de TrendTip.
- Debe velar por el mantenimiento de la confidencialidad, disponibilidad e integridad de los sistemas de Información. Se reúne de forma habitual mensualmente.
- Revisar y aprobar el programa de auditoría interna de la entidad.
- Revisar los informes emitidos por la auditoría interna de acuerdo con lo dispuesto en las normas.
- Considerar las observaciones de los auditores externos e internos sobre las debilidades de control interno encontradas durante la realización de sus tareas, así como las acciones correctivas implementadas por la Gerencia General, tendiente a regularizar o minimizar esas debilidades.
- Revisar periódicamente el cumplimiento de las normas de independencia de los auditores externos.

Auditor interno

El auditor interno, tal y como se ha definido en el procedimiento de auditoría interna, se trata de una figura externa a la organización. Los objetivos de auditor interno, son determinados por la dirección general; y entre sus actividades destacan:

- Crear un plan de auditoría.
- Establecer los criterios de evaluación.
- Seleccionar el método de evaluación apropiado.
- Realizar la evaluación de los controles implementado.
- Redactar un informe de auditoría con los hallazgos encontrados

Anexo G: Declaración de aplicabilidad

Tabla 27: Declaración de aplicabilidad

	Descripción	Aplica	Justificación	Evidencia o registro de implementación	Evidencia planificada
A.5	**Políticas de seguridad**				
A.5.1.1	Documento de la política de seguridad de la información.	Si	Por requisito de la ISO 27001 y GDPR se deben definir un conjunto de políticas que estén aprobadas por la dirección y comunicadas a los empleados	Política de seguridad de la información y Marco normativo	
A.5.1.2	Revisión de la política de seguridad de la información.	Si	Por requisito de la norma ISO 27001 y GDPR se adopta este control, puesto que las políticas se deben revisar a intervalos planificados, o si ocurren cambios significativos para asegurar su eficacias continua.	Actas de revisión periódica Control de cambios en la política de seguridad y en el marco normativo	
A.6	**Organización de la seguridad de la Información**				
A.6.1.1	Roles y responsabilidades en seguridad de la información	Si	Por requisito de GDPR, se deben definir los roles y responsabilidades en materia de seguridad de la información	Firma de la dirección de la política de seguridad y correo de aceptación de los roles y responsabilidades de las personas	
A.6.1.2	Segregación de tareas	Si	La organización es consciente de la importancia de la segregación de tareas, sin embargo, el tamaño de ella hace imposible segregar muchas de las funciones		Documento con los roles y responsabilidades

Tabla 27: Declaración de aplicabilidad

A.6.1.3	Contacto con las autoridades	Si	Los contactos con otras autoridades permiten a la Entidad anticiparse y prepararse para los posibles cambios en regulaciones y leyes		La organización es consciente de la importancia de tener un procedimiento donde se muestran los pasos a seguir para contactar con las autoridades, sin embargo, debido al tamaño de la organización todavía no se ha podido implantar
A.6.1.4	Contacto con grupos de interés especial	Si	La organización es consciente de la importancia de estar al día en noticias relativas a la ciberseguridad para poder hacer frente a las nuevas amenazas que surjan		La organización es consciente de la importancia de asistir a Foros con otras Entidades para estar al corriente de las novedades que pudieran aparecer, sin embargo, debido al tamaño de la organización todavía no se ha podido implantar
A.6.1.5	Seguridad de la información en la gestión de proyectos	Si	Por requisito de la ISO 27001, la seguridad de la información debe estar presente en todos los procesos del Sistema de Gestión incluyendo así los proyectos que se vayan a ejecutar	Política de seguridad de la información y Marco normativo	
A.6.2.1	Política de dispositivos móviles	Si	Se requiere de una política de dispositivos móviles donde se establezcan las acciones a realizar cuando los activos están fuera de las instalaciones de la Entidad	Política de dispositivos móviles	
A.6.2.2	Teletrabajo	No	TrendTip no cuenta con aplicaciones de teletrabajo		
A.7	**Seguridad relativa a los RRHH**				

Tabla 27: Declaración de aplicabilidad

A.7.1.1	Investigación de antecedentes	Si	Antes de contratar a una persona se debe mirar los antecedentes de la persona para asegurarse que ésta es apta para el cargo a desarrollar		Procedimiento de contratación personal
A.7.1.2	Términos y condiciones del empleo	Si	Por requisito de la norma ISO27001, es necesario la realización y firma de un acuerdo de confidencialidad		Acuerdo de confidencialidad y no divulgación de la información
A.7.2.1	Responsabilidades de gestión	Si	La dirección es consciente de sus responsabilidades en el sistema de gestión	Procedimiento de revisión por la dirección	
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Si	Por requisito de la norma ISO 27001, se adopta un plan de capacitación para la organización	Registro de asistencia a cursos de formación	
A.7.2.3	Proceso disciplinario	Si	Se requiere de un proceso disciplinario en caso de incumplimiento de los acuerdos establecidos	Cláusulas contractuales donde se establezca el proceso disciplinario en caso de incumplimiento.	

Tabla 27: Declaración de aplicabilidad

A.7.3.1	Responsabilidades ante la finalización o cambio	Si	La comunicación formal del cese de actividad de un empleado desencadenará las acciones oportunas para deshabilitar el acceso del usuario a los recursos de la empresa por cualquiera de los canales que estuvieran habilitados tanto físicos como lógicos. La información del usuario dado de baja se mantendrá hasta que se cumplan los plazos legales, para asegurar la capacidad de obtener evidencias frente a auditorías. El empleado devolverá todo el material suministrado por la Entidad para el acceso a los Sistemas de Información (portátil, token, tarjeta y otros similares)		Cláusulas contractuales sobre fuga de información donde se incluye la obligación de mantener la confidencialidad durante 6 meses después de la rescisión del contrato
A.8	**Gestión de activos**				
A.8.1.1	Inventario de activos	Si	Por requisito de GDPR y la norma ISO 27001, se requiere de un inventario de activos actualizado		Herramienta CMDB gestión de activos
A.8.1.2	Propiedad de los activos	Si	Por requisito de GDPR y la norma ISO 27001, se requiere de un inventario de activos en el que se incluya la propiedad de cada activo		Herramienta CMDB gestión de activos
A.8.1.3	Uso aceptable de los activos	Si	Por requisito de GDPR y la norma ISO 27001, los activos deben usarse acorde a las acciones del negocio	Actas de aceptación de los activos	
A.8.2.1	Directrices de clasificación	Si	Se debe identificar el valor de los activos para poner medidas acordes a su clasificación	Norma de gestión de activos	

Tabla 27: Declaración de aplicabilidad

A.8.2.2	Etiquetado y manejo de información	No	No se considera necesario el etiquetado de los activos por el escaso volumen que dispone la organización		
A.8.2.3	Manipulado de la información	Si	Se requiere definir proced		
A.8.3.1	Gestión de soportes extraíbles	No	No se permite la utilización de soportes extraíbles		
A.8.3.2	Eliminación de soportes	Si	Se requiere que los sistemas con información sensible sean eliminados para impedir el acceso a esa información	Albarán de destrucción de equipo	
A.8.3.3	Soportes físicos en tránsito	No	No se requiere transporte de información física		
A.9	**Control de acceso**				
A.9.1.1	Política de control de acceso	Si	Se debe establecer una política de acceso donde se detallen	Política de control de acceso	
A.9.1.2	Acceso a las redes y a los servicios de red	Si	Asignas los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso	Registro de acceso a las redes	
A.9.2.1	Registro y baja de usuario	Si	Por requisito de GDPR	Registro de acceso a los sistemas de información	
A.9.2.2	Provisión de acceso de usuario	Si	Se requiere de un procedimiento para asignar o revocar los derechos de acceso de los usuarios a los sistemas	Registro de acceso a los sistemas de información	
A.9.2.3	Gestión de privilegios de acceso	Si	Se define una serie de grupos que tendrán determinados accesos para cada tipo de información establecida	Registro de acceso a los sistemas de información	

Tabla 27: Declaración de aplicabilidad

A.9.2.4	Gestión de la información secreta de autenticación de usuarios	Si	Se requiere que los usuarios mantengan en secreto la información de autenticación con el fin de que personal no autorizado no pueda acceder a los sistemas de información	Registro de acceso a los sistemas de información	
A.9.2.5	Revisión de los derechos de acceso de usuario	Si	Se requiere revisar los derechos de acceso de forma regular	Registro de acceso a los sistemas de información	
A.9.2.6	Retirada o reasignación de los derechos de acceso	Si	Se requiere eliminar los permisos de acceso a los sistemas de información de aquellos usuarios que hayan cambiado de responsabilidades o no se encuentren ya en la organización.	Registro de acceso a los sistemas de información	
A.9.3.1	Uso de la información secreta de autenticación	Si	Se requiere que los usuarios realicen buen uso de la información secreta de autenticación	Norma gestión de activos	
A.9.4.1	Restricción del acceso a la información	Si	El acceso a las aplicaciones y sistemas debe estar restringida a los perfiles autorizados	Norma gestión de activos	
A.9.4.2	Procedimientos seguros de inicio de sesión	Si		Norma gestión de activos	
A.9.4.3	Sistema de gestión de contraseñas	Si	Se precisa de una política de contraseñas, donde se establezcan los criterios de creación de contraseñas robustas	Norma gestión de activos	
A.9.4.4	Uso de utilidades con privilegios del sistema	Si	Se precisa la la elaboració		
A.10	**Criptografía**				

Tabla 27: Declaración de aplicabilidad

A.10.1.1	Política de uso de controles criptográficos	Si	Se precisa la contratación de un servicio de gestión de claves criptográficas para proteger la información almacenada	Contrato con el proveedor servicios en la nube del servicio de gestión de claves criptográficas	
A.10.1.2	Gestión de claves	Si	Se precisa la contratación de un servicio de gestión de claves criptográficas para proteger la información almacenada	Contrato con el proveedor servicios en la nube del servicio de gestión de claves criptográficas	
A.11	**Seguridad física y del entorno**				
A.11.1.1	Perímetro de seguridad física	Si	Se requiere de medidas de seguridad física para proteger los activos de la empresa	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a seguridad física	
A.11.1.2	Controles físicos de entrada	Si	Se requiere de controles de acceso a las instalaciones de la empresa	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a seguridad física	
A.11.1.3	Seguridad de oficinas, despachos y recursos	Si	Se requiere de controles de acceso a las instalaciones de la empresa	Registro del control de acceso a la oficina	
A.11.1.4	Protección contra amenazas externas y ambientales	Si	Se requiere de la implementación de medidas físicas que protejan a la Entidad frente amenazas externas y ambientales	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a protección frente a amenzas externas	
A.11.1.5	El trabajo en áreas seguras	Si	Se requiere de la implementación de medidas físicas que protejan a la Entidad frente amenazas externas y ambientales	Implementación de medidas físicas y procedimentales. Tener contacto con las autoridades.	
A.11.1.6	Áreas de carga y descarga	No	No se dispone de un área de carga y descarga		

Tabla 27: Declaración de aplicabilidad

A.11.2.1	Emplazamiento y protección de equipos	Si	Se requiere que los sistemas de información se encuentren ubicados en zonas en las que se reduzcan las amenazas y riesgos ambientales.	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a seguridad física	
A.11.2.2	Instalaciones de suministro	Si	Se requiere que los sistemas de información estén protegidos frente a fallos de alimentación	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a seguridad física	
A.11.2.3	Seguridad del cableado	Si	Se requiere que el cableado de los sistemas de información esté protegido frente a daños o interceptaciones	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a seguridad física	
A.11.2.4	Mantenimiento de los equipos	Si	Se requiere de un mantenimiento de los equipos para asegurarse de su disponibilidad e integridad	Ejecución de contratos sobre equipos informáticos incluyendo mantenimientos preventivos y de soporte.	
A.11.2.5	Retirada de materiales propiedad de la empresa	Si	Se requiere de un procedimiento donde se especifiquen las pasos a seguir a la hora de destruir activos obsoletos	Apartado de la política de gestión de activos relativo a destrucción de soportes físicos	
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Si	Se requiere la aplicación de medidas de seguridad para aquellos equipos que se encuentran fuera de las instalaciones de la organización	Clausulado del contrato con el proveedor de servicios en la nube donde se especifican los requerimientos relativos a seguridad física	
A.11.2.7	Reutilización o eliminación segura de equipos	Si	Se requiere de un procedimiento formal donde se especifique los pasos para la eliminación segura de equipos		Procedimiento eliminación segura de equipos
A.11.2.8	Equipo de usuario desatendido	Si	Para evitar posibles incidentes de seguridad, es necesario concienciar a los empleados para evitar que dejen el equipo desatendido	Apartado del curso de capacitación de seguridad en el que se incluye un apartado de bloqueo de ordenador	

Tabla 27: Declaración de aplicabilidad

A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Si	Para evitar posibles incidentes de seguridad, es necesario concienciar a los empleados para que mantengan su escritorio limpio a la hora de finalizar su trabajo diario		En el curso de capacitación de seguridad en el que se incluya un apartado de puesto despejado y pantalla limpia
A.12	**Gestión de las comunicaciones y operaciones**				
A.12.1.1	Documentación de procedimientos de operación	Si	Se requiere se documenten procedimientos de operación que incluyan: copias de respaldo, mantenimiento de equipos. gestión de soportes, gestión de salas de ordenadores...	Procedimiento de operación	
A.12.1.2	Gestión de cambios	Si	Se mantendrá un control continuo de cambios realizados en el sistema, de forma que se puedan planificar para reducir el impacto sobre la prestación de los servicios afectados y determinar si los cambios son relevantes para la seguridad del sistema.		Procedimiento de gestión de cambios y designación de los roles y responsabilidades
A.12.1.3	Gestión de capacidades	Si	Con carácter previo a la puesta en explotación, se realizará un estudio previo para mirar las necesidades de procesamiento. y las necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.		Procedimiento de gestión de capacidades y designación de los roles y responsabilidades
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	No	El servicio se encuentra externalizado		

Tabla 27: Declaración de aplicabilidad

A.12.2.1	Controles contra el código malicioso	Si	Se requiere de programas que analicen la información en busca	Programa de análisis de malware	
A.12.3.1	Copias de seguridad de la información	Si	Se requiere de un política de backup para mantener la integridad y la disponibilidad de la información	Registro con los últimos backup realizados	Política de backup
A.12.4.1	Registro de eventos	Si	Se requiere que todos los eventos que ocurren dentro de la empresa deben ser registrados y verificados	Consola de monitorización de logs	
A.12.4.2	Protección de la información de registro	Si	Se requiere que los logs recogidos estén adecuadamente protegidos para garantizar la integridad de la información	Consola de monitorización de logs	
A.12.4.3	Registro de administración y operación	Si	Se requiere que los registros de actividad de los perfiles de administrador	Consola de monitorización de logs	
A.12.4.4	Sincronización del reloj	Si	Se requiere sincronizar los relojes de las máquinas para evitar que se obtengan registros a distintas horas		
A.12.5.1	Instalación de software en explotación	Si	Únicamente el software elegido por la empresa debe ser instalado	Listado de Sw autorizado	
A.12.5.2	Gestión de vulnerabilidades técnicas	Si	Se deben gestionar las vulnerabilidades encontradas en la organización con el fin de garantizar que la organización no se encuentra expuesta a ellas	Reporte mensual de vulnerabilidades encontradas y solucionadas	
A.12.5.3	Restricción en la instalación de software	Si	Únicamente el software elegido por la empresa debe ser instalado	Listado de Sw autorizado	

Tabla 27: Declaración de aplicabilidad

A.12.5.4	Controles de auditoría de sistemas de información	Si	Se requiere de una planificación de los controles de auditoría con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio	Plan de auditoría	
A.13	**Seguridad de las comunicaciones**				
A.13.1.1	Controles de red	Si	Es necesario controlar el tráfico que circula por la red para evitar fugas de información	Diagrama de red de la Entidad	
A.13.1.2	Seguridad de los servicios de red	Si	Se han establecido SLAs con el proveedor de servicios para verificar que los recursos de red se están gestionando de la manera correcta	Se cuenta con informes mensuales de los servicios firewall, WAN y LAN realizados por los proveedores.	
A.13.1.3	Segregación de redes	Si	Las redes se encuentran segregadas para acotar el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren	Diagrama de red de la Entidad	
A.13.2.1	Políticas y procedimientos de intercambio de información	Si	Por requisito de la ISO 27001, se deben elaborar y documentar políticas y procedimientos de intercambio de la información	Política de operaciones	
A.13.2.2	Acuerdos de intercambio de información	Si	Por requisito de la ISO 27001, se deben elaborar acuerdos de intercambio de la información	Control de sesiones en equipos.	
A.13.2.3	Mensajería electrónica	Si	Se requiere que las comunicaciones por correo se encuentren cifradas	DLP mensajería electrónica	

Tabla 27: Declaración de aplicabilidad

A.13.2.4	Acuerdos de confidencialidad o no revelación	Si	Se requiere de acuerdos de confidencialidad donde	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).	
A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**				
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No	Servicio externalizado		
A.14.1.2	Asegurar a los servicios de aplicaciones en redes públicas	No	Servicio externalizado		
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	No	Servicio externalizado		
A.14.2.1	Política de desarrollo seguro	No	Servicio externalizado		
A.14.2.2	Procedimiento de control de cambios en sistemas	No	Servicio externalizado		
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No	Servicio externalizado		
A.14.2.4	Restricciones a los cambios en los paquetes de software	Si	La entidad considera necesaria la implantación d una política que evite la modificación de sw de terceros en casos no necesarios	Marco normativo	
A.14.2.5	Principios de ingeniería de sistemas seguros	No	Servicio externalizado		
A.14.2.6	Entorno de desarrollo seguro	No	Servicio externalizado		

Tabla 27: Declaración de aplicabilidad

A.14.2.7	Externalización del desarrollo de software	Si	El desarrollo de la página web de Trendtip se encuentra externalizado	Contrato con empresa externa de desarrollo sw	
A.14.2.8	Pruebas funcionales de seguridad de sistemas	No	Servicio externalizado		
A.14.2.9	Pruebas de aceptación de sistemas	No	Servicio externalizado		
A.14.3.1	Protección de los datos de prueba	No	Servicio externalizado		
A.15	**Relación con proveedores**				
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Si	Por requisito de GDPR y la norma ISO 27001, es necesaria la elaboración de una política de seguridad en la relación con los proveedores.		Norma de gestión de proveedores actualizada y firmada por la alta dirección
A.15.1.2	Requisitos de seguridad en contratos con terceros	Si	Por requisito de GDPR, se deben establecer una serie de requisitos de seguridad en los contratos con los proveedores.	Cláusulas contractuales de los contratos con los proveedores.	
A.15.1.3	Cadena de suministros de tecnología de la información y de las comunicaciones	Si	Los contratos con proveedores deben establecer los requerimientos de seguridad para hacer frente a los riesgos de seguridad	Cláusulas contractuales de los contratos con los proveedores.	
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Si	Por requisito de la ISO 27001, se debe realizar un seguimiento de la gestión de servicios que realizan los proveedores	SLA del servicio	
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Si	Por requisito de la ISO 27001, se deben gestionar los cambios en las provisiones de servicio		Plan de gestión del conocimiento donde se identifiquen y documenten todos aquellos procesos críticos de la Entidad

Tabla 27: Declaración de aplicabilidad

A.16	**Gestión de incidentes de seguridad de la información**	**Si**			
A.16.1.1	Responsabilidades y procedimientos	Si	Por requisito de GDPR se deben establecer procedimiento donde se definan el plan de actuación en caso de incidente así como los roles y responsabilidades que participan	Apartado del procedimiento de gestión de incidentes donde se incluye las responsabilidades del área de los incidentes de seguridad.	Apartado del procedimiento de gestión de incidentes donde se incluye las responsabilidades del área de los incidentes de seguridad.
A.16.1.2	Notificación de los eventos de seguridad de la información	Si	Por requisito de la norma ISO 27001, se deben establecer los canales mediante los cuales se notifican los incidentes de seguridad		Procedimiento de gestión de incidentes
A.16.1.3	Notificación de puntos débiles de la seguridad	Si	Por requisito de la norma ISO 27001, se deben establecer los canales mediante los cuales se notifican los incidentes de seguridad		Procedimiento de gestión de incidentes
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Si	Por requisito de la norma ISO 27001, los incidentes de seguridad deben clasificarse en función de los criterios establecidos en la norma de gestión de incidentes.		Procedimiento de gestión de incidentes
A.16.1.5	Respuesta a incidentes de seguridad de la información	Si	Por requisito de la norma ISO 27001, los incidentes de seguridad deben clasificarse en función de los criterios establecidos y llevar a cabo las acciones oportunas en función de su criticidad		Procedimiento de gestión de incidentes

Tabla 27: Declaración de aplicabilidad

A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Si	La dirección establece la necesidad de que los planes de respuesta se actualicen con las lecciones aprendidas para evitar que estos puedan volver a suceder		Plan de respuesta a incidentes actualizado con las últimas lecciones aprendidas
A.16.1.7	Recopilación de evidencias	Si	Se deben establecer los procedimientos para garantizar una rápida respuesta, efectiva y adecuada a los incidentes de seguridad		Procedimiento de análisis forense
A.17	**Aspectos de segruidad de la información para la gestión de la continuidad del negocio**				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Si	La dirección establece la necesidad de realizar un calendario de pruebas para verificar que los sistemas están disponibles de acuerdo a los criterios establecidos en la norma de gestión de la continuidad del negocio.		Calendario con las pruebas de continuidad
A.17.1.2	Implementar la continuidad de la seguridad de la información	Si	Por requisito de la norma ISO 27001 y GDPR, se debe implantar un plan de continuidad en caso de incidente de seguridad, de modo que asegure la disponibilidad de los recursos.		Calendario con las pruebas de continuidad

Tabla 27: Declaración de aplicabilidad

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si	La dirección establece la necesidad de realizar un calendario de pruebas para verificar que los sistemas están disponibles de acuerdo a los criterios establecidos en la norma de gestión de la continuidad del negocio.		Plan de continuidad del negocio actualizado con las lecciones aprendidas
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Si	Se requiere de un sistema redundado para obtener la máxima disponibilidad posible	Contrato con el proveedor servicios en la nube	
A.18	**Cumplimiento**				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Si	Por requerimiento de la norma ISO 27001, se deben identificar las leyes aplicables y establecer los controles apropiados para su cumplimiento	Documento con las leyes aplicables en el SGSI	
A.18.1.2	Derechos de propiedad intelectual	Si	Por requerimiento de la norma ISO 27001	Documento con las leyes aplicables en el SGSI	
A.18.1.3	Protección de los registros de la organización	Si	Por requerimiento de la norma ISO 27001	Procedimiento de control de acceso sobre sistemas de información y aplicaciones	
A.18.1.4	Protección y privacidad de la información de carácter personal	Si	Por requerimiento de la norma ISO 27001	Documento con las leyes aplicables en el SGSI	
A.18.1.5	Regulación de los controles criptográficos	Si	Por requerimiento de la norma ISO 27001	Documento con las leyes aplicables en el SGSI	
A.18.2.1	Revisión independiente de la seguridad de la información	Si	Por requerimiento de la norma ISO 27001	Programa anual de auditoría	
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Si	Por requerimiento de la norma ISO 27001	Programa anual de auditoría	

Tabla 27: Declaración de aplicabilidad

A.18.2.3	Comprobación del cumplimiento técnico	Si	Por requerimiento de la norma ISO 27001	Programa anual de auditoría	

Anexo H: Inventario de activos

Tabla 28: Inventario y clasificación de activos

ID	Activo	Descripción	Ámbito	Activos esenciales
ID_01	Oficina	Planta de un edificio de oficinas donde se encuentra situada la sede de la empresa	Instalaciones	No
ID_02	Ordenadores personales x 3	Ordenadores Dell	Hardware	No
ID_03	Ordenador	Ordenador Mac	Hardware	No
ID_04	Impresora	RICOH MP 2555ASP	Hardware	No
ID_05	Teléfonos x 4	Samsung Galaxy J7	Hardware	No
ID_06	Cámara fotográfica	Canon + adaptador de montura EF-EOS R	Hardware	No
ID_07	Router	Linksys EA6900-EJ – Router inalámbrico Smart Wi-Fi de doble banda AC1900	Hardware	No
ID_08	Switch	NETGEAR Nighthawk SX10	Hardware	No
ID_09	Firewall	Sophos XG 750	Hardware	No
ID_10	Máquina virtual RedHat x2	Licencia RedHat para el servidor web de AWS	Aplicación	Si
ID_11	Windows Profesional 10	Liciencia windows para los ordenadores Dell	Aplicación	No
ID_12	MACos Mojave	Licencia MacOS para el ordenador Machintosh	Aplicación	No
ID_13	Adobe Photoshop	Liciencia de photoshop para la realización de fotos a nuevas tendencias	Aplicación	No
ID_14	Java Enterprise	Software utilizado para el desarrollo de la página web de TrendTip	Aplicación	No
ID_15	Antivirus	Kaspersky endpoint security	Aplicación	No
ID_16	Microsoft Office	Microsoft Office	Aplicación	No

Tabla 28: Inventario y clasificación de activos

ID_17	Servidor web x2	Tomcat	Aplicación	Si
ID_18	Código fuente	Código fuente aplicación TrendTip	Datos	Si
ID_19	Contratos con proveedores	Contratos con los proveedores de servicios IasS y SaaS	Datos	Si
ID_20	BBDD de clientes	Contratos y datos de los diferentes proveedores de ropa con los que trabaja TrendTip	Datos	Si
ID_21	BBDD empleados	Nóminas y datos personales de los empleados de TrendTip	Datos	Si
ID_22	BBDD aplicación	Datos de aplicación	Datos	Si
ID_23	Resultados de los análisis de tendencias	Informes y resultados de los análisis de tendencia realizados	Datos	Si
ID_24	Contenido audiovisual	Contenido audiovisual para campañas de marketing	Datos	Si
ID_25	Copias de respaldo de la BBDD	Copias de respaldo de la BBDD	Datos	Si
ID_26	Ficheros configuración de los sistemas	Ficheros configuración de los sistemas	Datos	Si
ID_27	Logs de acceso a los sistemas	Logs de acceso a los sistemas	Datos	Si
ID_28	Red local	Red LAN	Red	No
ID_29	Servicio de proveedor de servios SaaS	Servicio de correo electrónico y ofimático ofrecido por Google	Servicio	Si
ID_30	Servicio de proveedor de servicios IaaS	Servicio de IaaS dado por AWS	Servicio	Si
ID_31	Servicio de BBDD como servicio	Servicio de Aurora SQL ofrecido por AWS	Servicio	Si
ID_32	Sistemas de alimentación	Cableado para el suministro de electricidad de la oficina	Equipamiento auxiliar	No
ID_33	CCTV	Sistema de videovigilancia	Equipamiento auxiliar	No

Tabla 28: Inventario y clasificación de activos

ID_34	Equipos de climatización	Aire Acondicionado Split Panasonic Kit UE9-RKE	Equipamiento auxiliar	No
ID_35	CEO	Director de la empresa TrendTip	Personal	Si
ID_36	Responsable IT	Persona encargada de la parte de tecnología y sistemas de TrendTip	Personal	Si
ID_37	Responsable de marketing	Persona responsable de las campañas de marketing de TrendTip	Personal	Si
ID_38	Responsable de ventas	Persona responsable de ventas y contratos con proveedores	Personal	Si
ID_39	Desarrollar página web	Personal externo para el desarrollo de la página web de TrendTip	Personal	Si

Anexo I: Impacto de los activos la materialización de las amenazas

Tabla 29: Valoración del impacto en las instalaciones

ACTIVO: Instalaciones	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
Oficina				**50%**	**100%**	
[N.1] Fuego	1/100				100%	
[N.2] Daños por agua	1/100				100%	
[N.*] Desastres naturales	1/100				100%	
[I.1] Fuego	1/100				100%	
[I.2] Daños por agua	1/100				100%	
[I.*] Desastres industriales	1/100				100%	
[I.6] Corte del suministro eléctrico	1/10			50%		

Tabla 30: Valoración del impacto en el Hardware

ACTIVO: Hardware	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
Ordenadores personales x 3			**100%**	**100%**	**100%**	
Ordenador			**100%**	**100%**	**100%**	
Impresora			**100%**	**100%**	**100%**	
Teléfonos x 4			**100%**	**100%**	**100%**	
Cámara fotográfica			**100%**	**100%**	**100%**	
Router			**100%**	**100%**	**100%**	
Switch			**100%**	**100%**	**100%**	
Firewall			**100%**	**100%**	**100%**	
[N.1] Fuego	1/100				100%	
[N.2] Daños de agua	1/100				100%	
[I.1] Fuego	1/100				100%	
[I.2] Daños de agua	1/100				100%	
[I.*] Desastres naturales	1/100				100%	
[I.3] Contaminación mecánica	1/100				100%	
[I.5] Avería de origen físico	1/10				100%	

Tabla 30: Valoración del impacto en el Hardware

[I.6] Cortes de suministro	1/100				100%	
[I.7] Condiciones inadecuadas de temperatura o humedad	1/100				100%	
[E.2] Errores del administrador	1/10		100%	100%	100%	
[A.6] Abuso de privilegios de acceso	1/10		80%	20%	20%	
[A.7] Uso no previsto	1		50%	50%	10%	
[A.11] Acceso no autorizado	1/10		100%	100%		
[A.23] Manipulación de los equipos	1/100		50%		50%	
[A.24] Denegación de servicio	1/100				10%	
[A.25] Robo	1/100		50%		50%	
[A.26] Ataque destructivo	1/100				50%	

Tabla 31: Valoración del impacto en los datos

ACTIVO: Datos	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Código fuente		**100%**	**100%**	**100%**	**100%**	
Contratos con proveedores		**100%**	**100%**	**100%**	**100%**	
BBDD de clientes		**100%**	**100%**	**100%**	**100%**	
BBDD empleados		**100%**	**100%**	**100%**	**100%**	
Contenido audiovisual		**100%**	**100%**	**100%**	**100%**	
Resultados análisis de tendencias		**100%**	**100%**	**100%**	**100%**	
Copias de respaldo de la BBDD		**100%**	**100%**	**100%**	**100%**	
Ficheros configuración de los sistemas		**100%**	**100%**	**100%**	**100%**	
Logs de acceso a los sistemas		**100%**	**100%**	**100%**	**100%**	
[E.1] Errores de los usuarios	10		20%	20%	40%	
[E.2] Errores del administrador	1/10		40%	40%	60%	

Tabla 30: Valoración del impacto en el Hardware

[E.15] Alteración accidental de la información	1/100			30%		
[E.18] Destrucción de la información	1/10			50%		
[E.19] Fugas de información	1/10			30%		
[A.5] Suplantación de la identidad del usuario	1/100	100%	80%	60%		
[A.6] Abuso de privilegios de acceso	1/100		80%	30%	30%	
[A.15] Modificación de información	1/100			100%		
[A.18] Destrucción de la información	1/100				100%	
[A.19] Divulgación de información	1/100		100%			

Tabla 32: Valoración del impacto en las aplicaciones

ACTIVO: Aplicación	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
Windows Server		**100 %**	**100 %**	**100 %**	**100 %**	
Windows Profesional 10		**100 %**	**100 %**	**100 %**	**100 %**	
MACos Mojave		**100 %**	**100 %**	**100 %**	**100 %**	
Adobe Photoshop		**100 %**	**100 %**	**100 %**	**100 %**	
Java Enterprise		**100 %**	**100 %**	**100 %**	**100 %**	
Antivirus		**100 %**	**100 %**	**100 %**	**100 %**	
Microsoft Office		**100 %**	**100 %**	**100 %**	**100 %**	
Máquina virtual RedHat x2		**100 %**	**100 %**	**100 %**	**100 %**	
Servidor web x2		**100 %**	**100 %**	**100 %**	**100 %**	
[I.5] Avería de origen físico	1/10				50 %	
[E.1] Errores de los usuarios	1		10 %	20 %	30 %	
[E.2] Errores del administrador	1		80 %	60 %	60 %	
[E.8] Difusión de sw dañino	1/10		50 %	50 %	30 %	

Tabla 32: Valoración del impacto en las aplicaciones

[E.9] Errores de encaminamiento	1/100		60 %			
[E.10] Errores de secuencia	1/100			20 %		
[E.15] Alteración accidental de la información	1/100		60 %			
[E.18] Destrucción de la información	1/100				50 %	
[E.19] Fugas de información	1/100		80 %			
[E.20] Vulnerabilidades de los programas	1/10		30 %	30 %	50 %	
[E.21] Errores de mantenimiento/actualización de programas	10			30 %	50 %	
[A.5] Suplantación de la identidad del usuario	1/100	100 %	80 %	80 %		
[A.6] Abuso de privilegios de acceso	1/100		60 %	30 %	30 %	
[A.7] Uso no previsto	1/100		10 %	20 %	20 %	
[A.8] Difusión de sw dañino	1/10		80 %	80 %	100 %	
[A.9] Encaminamiento de mensajes	1/100		40 %			
[A.10] Alteración de secuencia	1/100			40 %		
[A.11] Acceso no autorizado	1/100		90 %	80 %		
[A.15] Modificación de información	1/100			100 %		
[A.18] Destrucción de la información	1/100				100 %	
[A.19] Divulgación de información	1/100		100 %			
[A.22] Manipulación de programas	1/110		60 %	60 %	60 %	

Tabla 33: Valoración del impacto en los servicios

ACTIVO:Servicios	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**

Tabla 33: Valoración del impacto en los servicios

Servicio de proveedor de servicios SaaS			**100 %**	**100 %**	**100 %**	**100 %**
Servicio de proveedor de servicios IaaS			**100 %**	**100 %**	**100 %**	**100 %**
Servicio de BBDD como servicio			**100 %**	**100 %**	**100 %**	**100 %**
[E.1] Errores de los usuarios	1/10		30 %	30 %	30 %	
[E.2] Errores del administrador	1/100		50 %	50 %	50 %	
[E.9] Errores de los usuarios	1/10		40 %			
[E.10] Errores de secuencia	1/100			30 %		
[E.15] Alteración accidental de la información	1/100			80 %		
[E.18] Destrucción de la información	1/100			80 %		
[E.19] Fugas de información	1/100				50 %	
[E.24] Caída del sistema por agotamiento de recursos	1/100				50 %	
[A.5] Suplantación de la identidad del usuario	1/100		30 %	30 %	30 %	
[A.6] Abuso de privilegios de acceso	1/100		20 %	30 %	30 %	
[A.7] Uso no previsto	1/100		30 %			
[A.9] Encaminamiento de mensajes	1/100			20 %		
[A.10] Alteración de secuencia	1/100			20 %		
[A.11] Acceso no autorizado	1/100			70 %	30 %	
[A.13] Repudio	1/100					100 %
[A.15] Modificación de información	1/100			100 %		
[A.18] Destrucción de la información	1/100				100 %	
[A.19] Divulgación de información	1/100		100 %			

Tabla 33: Valoración del impacto en los servicios

[A.24] Denegación de servicio	1/100				100 %	

Tabla 34: Valoración del impacto en las redes

ACTIVO: Redes	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
Red local				100%	100%	100%
[I.8] Fallo de servicios de comunicaciones	1/100				100%	
[E.2] Errores del administrador	1/10		30%	40%	50%	
[E.9] Errores de los usuarios	1/100		30%			
[E.10] Errores de secuencia	1/100			40%		
[E.15] Alteración accidental de la información	1/100			40%		
[E.18] Destrucción de la información					80%	
[E.19] Fugas de información	1/100		30%			
[E.24] Caída del sistema por agotamiento de recursos					50%	
[A.5] Suplantación de la identidad del usuario	1/100	100%	50%	30%		
[A.6] Abuso de privilegios de acceso	1/100		30%	30%	30%	
[A.7] Uso no previsto	1/100		30%	30%	50%	
[A.9] Encaminamiento de mensajes	1/100		50%			
[A.10] Alteración de secuencia	1/100			50%		
[A.11] Acceso no autorizado	1/100			50%		
[A.12] Análisis de tráfico	1/100		30%			
[A.15] Interceptación de información			80%			

Tabla 34: Valoración del impacto en las redes

[A.15] Modificación de información	1/100			100%		
[A.19] Divulgación de información	1/100		100%			
[A.24] Denegación de servicio					100%	

Tabla 35: Valoración del impacto en los sistemas de equipamiento auxiliar

ACTIVO: Sistemas de equipamiento auxiliar	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Sistemas de alimentación			20%	10%	100%	100%
CCTV			20%	10%	100%	100%
Equipos de climatización			20%	10%	100%	
[N.1] Fuego	1/100				100%	
[N.2] Daños por agua	1/100				100%	
[N.*] Desastres naturales	1/100				100%	
[I.1] Fuego	1/100				100%	
[I.2] Daños por agua	1/100				100%	
[I.3] Contaminación mecánica	1/100				100%	
[I.4] Contaminación electromagnética	1/100				100%	
[I.5] Avería de origen físico o lógico	1/100				100%	
[I.7] Condiciones inadecuadas de temperatura o humedad	1/100				100%	
[I.9] Fallo de servicios de comunicaciones	1/10				100%	
[E.23] Errores de mantenimiento/actualización de equipos	1/10				100%	
[E.25] Pérdida de equipos	1/100		20%		100%	

Tabla 35: Valoración del impacto en los sistemas de equipamiento auxiliar

[A.7] Uso no previsto	1/100		20%	10%	30%	
[A.11] Acceso no autorizado	1/100		20%	10%		
[A.23] Manipulación de los equipos	1/100		20%		100%	
[A.25] Robo	1/100		20%		100%	
[A.26] Ataque destructivo	1/100				100%	

Tabla 36: Valoración del impacto en el personal

ACTIVO: Personal	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
CEO		**50%**	**50%**	**50%**	**100%**	**50%**
Responsable IT		**50%**	**50%**	**50%**	**100%**	**50%**
Responsable de marketing		**50%**	**50%**	**50%**	**100%**	**50%**
Responsable de ventas		**50%**	**50%**	**50%**	**100%**	**50%**
Desarrollador página web		**50%**	**50%**	**50%**	**100%**	**50%**
[E.28] Indisponibilidad del personal	1				100%	
[A.28] Indisponibilidad del personal	1/10				100%	
[A.29] Extorsión	1/100	50%	50%	50%		50%
[A.29] Ingeniería social	1/100	50%	50%	50%		50%

Anexo J: Proyectos para reducir el riesgo de la organización

Tabla 37: Proyecto 1 - Plan de continuidad del negocio o plan de contingencia

Plan de continuidad del negocio o plan de contingencia.
Dominio ISO: A.17: Aspectos de seguridad de la información para la gestión de la continuidad del negocio
Objetivo: Definir una serie de mecanismos y medidas que aseguren la disponibilidad de los servicios críticos de los que dispone la organización con el objetivo de reducir el impacto de los incidentes en la imagen de la organización
Descripción: El plan de continuidad del negocio debe contar con los siguientes aspectos: • Identificar los activos que intervienen en los procesos de negocio críticos de la organización. • Identificar aquellos eventos que puedan causar indisponibilidad en los servicios, la frecuencia con la que se pueden producir y sus efectos y consecuencias. • Desarrollar un plan para garantizar la disponibilidad de la información en el nivel y tiempo requerido. • Llevar a cabo pruebas de continuidad del negocio. • Contratar una póliza de seguro ante incidentes de seguridad.

Tabla 37: Proyecto 1 - Plan de continuidad del negocio o plan de contingencia

Planificación:

Fase I: Identificación y análisis del negocio y los procesos críticos de la organización mediante la realización de un BIA (Business Impact Analysis)

En esta fase se debes determinar cuales son los objetivos de negocio y los procesos que se consideran críticos para el funcionamiento de la compañía y en función de ellos analizar cuáles son los riesgos asociados a dichos procesos para identificar cuáles son las causas potenciales que pueden llegar a interrumpir un negocio.

Fase II – Selección de estrategias

Esta fase tiene dos objetivos:

- Valorar las diferentes alternativas y estrategias de respaldo en función de los resultados obtenidos en la fase anterior, para seleccionar la más adecuada a las necesidades de la compañía.
- Corregir las vulnerabilidades detectadas en el Análisis de Riesgos.

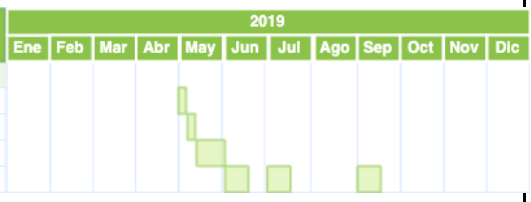
· ***Fase III- Desarrollo del plan***

Una vez que se ha seleccionado la estrategia, se debe desarrollarla e implantarla dentro de la compañía. En esta fase se desarrollan los procedimientos y planes de actuación para las distintas áreas y equipos, y se organizan los equipos que intervienen en cada fase del Plan.

· ***Fase IV – Pruebas y mantenimiento***

Esta última fase tiene como objetivo verificar que el plan realizado realmente funciona y es efectivo. Para ello se define la estrategia de pruebas y así ir afinándolo según los resultados obtenidos.

	Proyectos	Duración	Comienzo
PR1	**Plan de Continuidad del negocio**		06.05.19
Fase 1	BIA	2 días	06.05.19
Fase 2	Selección de estrategias	1 día	08.06.19
Fase 3	Definir y desarrollar el plan de continuidad	5 días	09.05.19
Fase 4	Pruebas que garanticen la efectividad	2 horas/prueba	01.06.19



Personal: Se ha optado por la contratación de un consultor externo para la implantación de este plan con unos honorarios de 50 euros/hora

Coste: El coste derivado del servicio asciende a 3100 euros/año.

Beneficios:

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones además de su impacto económico y reputacional sobre la organización.
- Permite conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Minimizar o atenuar las pérdidas para el negocio en caso de desastre.
- Identifica y clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.
- Fomenta e implica a los recursos humanos de la compañía en las actividades de continuidad.

Riesgos a mitigar: Indisponibilidad de la aplicación de TrendTip

Tabla 38: Proyecto 2 - Plan de concienciación

Plan de concienciación.
Dominio ISO: A7.2: Seguridad relativa a los RRHH, A12 Seguridad en las operaciones
Objetivo: Concienciar a los empleados de TrendTip sobre los procedimientos y políticas de seguridad, así como el buen uso de los recursos para mantener y mejorar los niveles de seguridad a los que está expuesta la organización.
Descripción: El plan de concienciación contará con dos subproyectos, un programa de concienciación y un curso. El **programa de concienciación** se va a realizar en las siguientes etapas: · ***Fase I: Evaluación del nivel de concienciación*** de los empleados de la organización mediante la realización de ataques dirigidos (por ejemplo, correo electrónico malicioso o pendrive con contenido malicioso). · ***Fase II: Presentación de los resultados a la dirección*** · ***Fase III: Distribución y elaboración del material de concienciación***. Este debe estar enfocado en los siguientes 4 ámbitos: o La Información: tratamiento de la información sensible que maneja y genera la empresa, desde el punto de vista de la seguridad. o Los soportes: medidas de seguridad a tener en cuenta y a aplicar en los diferentes soportes que utilizamos para trabajar con información corporativa, tanto dentro como fuera de la empresa. o El puesto de trabajo: medidas de seguridad y buenas prácticas a tener en cuenta y a aplicar en nuestro puesto de trabajo para que éste sea lo más seguro posible. o Los dispositivos móviles: medidas de seguridad y buenas prácticas a tener en cuenta y a aplicar en los dispositivos móviles que utilizamos para trabajar con información corporativa, tanto dentro como fuera de la empresa. Por otra parte, además de este programa se impartirá un **curso de seguridad** a los empleados en el que se expliquen las políticas de seguridad de la empresa.

Tabla 38: Proyecto 2 - Plan de concienciación

Planificación:

· Programa de formación de duración 1 semana en el que se desarrollarán las 3 fases descritas anteriormente:

- Fase 1: 10 horas
- Fase 2: 2 hora
- Fase 3: 12 horas

· Un curso de formación y concienciación con carácter anual y de duración 2 horas realizado por el responsable de seguridad IT de la empresa. Además de éste, el curso se impartirá también cada vez que se incorpore una persona nueva a la plantilla

	Proyectos	Duración	Comienzo	Septiembre 2019				
				9	10	11	12	13
PR1	**Programa de concienciación**	5 días	09.09.19					
Fase 1	Evaluación del nivel de concienciación	10 horas	09.09.19					
Fase 2	Presentación de los resultados de la evaluación	2 horas	10.09.19					
Fase 3	Distribución y redacción del material de seguridad	12 horas	11.09.19					

	Proyectos	Duración	Comienzo	2019											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
PR1	**Curso de concienciación**	2 horas	10.10.19												

Personal: Para el programa de formación se ha optado por la contratación de un consultor de seguridad externo, mientras que la impartición del curso y la elaboración del material es ejecutada por el responsable de TI.

Coste: El coste de prestación de servicios del consultor es de 50 euros/hora lo que asciende a un total de derivado del servicio externalizado asciende a 1200 euros/año.

Beneficios:

· Reducir los incidentes de seguridad de carácter humano y el impacto que tienen estos en la organización.

. Concienciar a los empleados para que sean capaces de tratar la información acorde a los niveles de seguridad estipulados, aplicar las medidas oportunas según los requisitos legales aplicables y estar plenamente informados de las políticas y procedimientos de seguridad de los que dispone la organización.

Riesgos a mitigar: Incidentes causados por falta de conocimiento del personal de TrendTip

Tabla 39: Proyecto 3 - Política de backups

Política de backups

Dominio ISO: A12.3 Copias de seguridad

Objetivo: Definir una política de backups que garantice la recuperación de los datos en caso de incidentes de seguridad y evite así tanto pérdidas económicas como reputacionales.

Descripción:

A día de hoy, en TrendTip se realizan copias de seguridad de los diferentes sistemas de los que dispone la organización, sin embargo, no se dispone de documentación dónde se defina este proceso. El proyecto consistirá en la redacción de una política de backups en la que se incluyan los siguientes aspectos:

Qué sistemas, BBDD deben disponer de copias de seguridad.

Con qué periodicidad se deben ejecutar dichas copias de seguridad.

Cuánto tiempo se deben guardar las copias de seguridad.

Quién es el encargado de realizar las copias de seguridad

Metodología a seguir

Planificación y personal:

Este proyecto será ejecutado por el responsable de TI de TrendTip y será un proyecto de corto alcance (3 días a jornada completa para la elaboración de dicha política)

No se requiere de ningún tipo de activo adicional para la ejecución del proyecto.

	Proyectos	Duración	Comienzo	Mayo 2019				
				20	21	22	12	13
PR1	Política de backup	3 días	20.05.19					

Coste: Incluido dentro de las tareas del responsable de IT

Beneficios:

· Minimizar o atenuar las pérdidas en caso de incidente

. Garantizar la recuperación de los datos en caso de incidente.

. Automatizar y securizar el almacenamiento de las copias de seguridad.

Riesgos a mitigar:

- Indisponibilidad de los servicios críticos

- Pérdida total de datos

Tabla 40: Proyecto 4 - Plan de control de cambios

Plan de control de cambios

Dominio ISO: A 12.1.2 Gestión de cambios

Objetivo: El proceso de Gestión de Cambios tiene como objetivo verificar que los cambios y modificaciones que se llevan a cabo en los sistemas de información están controlados y son revisados reduciendo así el impacto de dichas modificaciones en la disponibilidad de los servicios. Este proceso permite además efectuar los cambios de manera más eficiente, reduciendo duplicidades, solapamientos y errores.

Descripción:
Se va a desarrollar un procedimiento de gestión de cambios en el que se incluyen los siguientes aspectos:

- Registro de la solicitud del cambio. El registro debe contener información suficiente para que dicho cambio quede totalmente identificado (solicitante del cambio, motivo, etc.), con el fin de mantener un histórico de cambios.
- Revisión y autorización del cambio.
- Supervisión del cambio.
- Cierre del cambio.

Planificación:

- Fase 1: Elaboración del procedimiento de gestión de cambios
- Fase 2: Aprobación por la alta dirección del documento
- Fase 3: Comunicado de la elaboración del nuevo procedimiento a la organización y posterior distribución.

	Proyectos	Duración	Comienzo	Junio				
				L	M	X	J	V
PR1	Procedimiento gestión de cambios	3 días	10.06.19					

Personal: Será el responsable de TI el encargado de la redacción de este procedimiento. Se estima que en su realización tardará 3 días.

Coste: Incluido dentro de las tareas del responsable de IT

Beneficios:

- Ahorros en costes.
- Reducción del número de incidentes.
- Aumento de la productividad de la empresa
- Estandarización de procesos.
- - Mejorar la auditabilidad de los procesos

Riesgos a mitigar: indisponibilidad de la página web de TrendTip

Tabla 41: Proyecto 5 - Anonimización de las BBDD de clientes y empleados

Anonimización de las BBDD de clientes y empleados

Dominio ISO: A.10. Criptografía

Objetivo: El proceso de anonimización tiene como objetivo identificar y ocultar la información de carácter sensible contenida en la BBDD.

Descripción:

Durante este proceso se llevarán a cabo las siguientes fases:

- Fase 1: Evaluar los posibles riesgos que se pueden derivar de la anonimización.
- Fase 2: Determinar qué técnicas de anonimización van a ser las más adecuada.
- Fase 3: Velar por las medidas de seguridad necesarias para mantener la anonimización

Planificación y personal:

Fase 1: Será ejecutada por la persona responsable de TI de TrendTip. Se estima una duración de una semana para la realización del análisis de riesgos.

Fase 2: Se ha optado por la contratación de un consultor externo especializado para la ejecución de esta segunda fase con un sueldo de 50 euros/hora. A continuación se muestran cada una de las etapas que debe realizar el consultor así como el tiempo dedicado a cada uno de ellas y el coste asociado:

- Toma de requisitos: 3 horas (150 euros)
- Diseño de la solución: 5 horas (250 euros)
- Desarrollo de la solución: 10 horas (500 euros)
- Implantación: 6 horas (300 euros)

Fase 3: Al igual que la fase 1 será ejecutada por el responsable de TI de TrendTip. Se estima una duración de 40 horas para el diseño de medidas de seguridad que garanticen la anonimización de los datos.

	Proyectos	Duración	Comienzo	Junio 2019							
				17	18	19	20	21	24	25	26
	Anonimización BBDD	2 días	17.06.19								
Fase 1	Análisis de riesgos	16 horas	17.06.10								
	Evaluación y análisis de riesgos	16 horas	17.06.19								
Fase 2	Identificación usuarios potenciales de conocimiento	24 horas	19.06.19								
	Toma de requisitos	3 horas	19.06.19								
	Diseño solución	5 horas	19.06.19								
	Desarrollo de solución	10 horas	20.06.19								
	Implantación solución	6 horas	21.06.19								
Fase 3	Implementación de medidas de seguridad	24 horas	24.06.19								
	Implementación medidas	1 día	24.06.19								

Coste: En total, la ejecución del proyecto tiene un coste total para la empresa de 1200 euros por la contratación del servicio externalizado

Tabla 41: Proyecto 5 - Anonimización de las BBDD de clientes y empleados

Beneficios: · Minimizar o atenuar las pérdidas para el negocio en caso de intrusión y divulgación de los datos de la BBDD. . Cumplir con el reglamento europeo de protección de datos y la ley orgánica española.
Riesgos a mitigar: - Posibilidad de extraer de un conjunto de datos algunos registros que identifican a un empleado o cliente. - Posible Incumplimiento legal

Tabla 42: Proyecto 6 - Plan de gestión de incidentes

Plan de gestión de incidentes

Dominio ISO relacionado: A.16: Gestión de incidentes de seguridad de la información

Objetivo: Este proyecto tiene como objetivo proveer a la organización de diferentes procedimientos de gestión de incidentes acordes con la criticidad de sus actividades de negocio para garantizar el más rápido tratamiento.

Descripción:

Durante el proyecto se deben tratar los siguientes aspectos:

- Definir procedimientos formales de clasificación y escalado de incidentes de seguridad

- Definir procedimientos formales de comunicación de eventos de seguridad

Definir las personas responsables de la gestión de incidentes y puntos débiles de seguridad de forma efectiva una vez que se hayan comunicado.

Definir un procedimiento de lecciones aprendidas

Planificación y personal:

Este proyecto será ejecutado por el responsable de TI de TrendTip y será un proyecto de corto alcance (3 días)

No se requiere de ningún tipo de activo adicional para la ejecución del proyecto.

	Proyectos	Duración	Comienzo	Julio				
				L	M	X	J	V
PR1	Plan de gestión de incidentes	3 días	22.07.19					

Beneficios:

· Minimizar o atenuar las pérdidas para el negocio en caso de intrusión y divulgación de los datos de la BBDD.

. Garantizar la recuperación de los datos en caso de incidente.

Costes: Incluido dentro de las tareas del responsable de IT

Riesgos a mitigar:

- Indisponibilidad de los servicios críticos

Tabla 43: Proyecto 7 - Implementación de un servicio de monitorización

Implementación de un servicio de monitorización

Dominio ISO: A.14: Adquisición, desarrollo y mantenimiento de los procesos de soporte, A.12 Seguridad de las operaciones

Objetivo: El proceso de implementación de un servicio de monitorización tiene como objetivo verificar que los servidores web tienen las capacidades necesarias para prestar el servicio e identificar cuáles son los horarios más oportunos para el despliegue de nuevas versiones, además de detectar degradaciones de servicio y prevenir posibles incidencias.

Descripción:

Se va a implementar un servicio de monitorización en el que se incluyan los siguientes servicios:

Pruebas a nivel de servicio

Pruebas a nivel de máquina

Pruebas “Happy path”.

Recolección de métricas para identificar posibles eventos de seguridad (memoria, uso de disco, uso de red)

Planificación:

· Fase 1: Diseño de los planes de pruebas

· Fase 2: Implementación de los pruebas

· Fase 3: Implementación de medidas de recolección de métricas.

· Fase 4: Integración con herramientas de monitorización.

	Proyectos	Duración	Comienzo	Julio 2019				
				L	M	X	J	V
	Implementación de servicio de monitorización	5 días	03.06.19					
Fase 1	Diseño de los planes de prueba	6 horas	03.06.19					
Fase 2	Implementación de las pruebas	10 horas	03.06.19					
Fase 3	Implementación de medidas de recolección de métricas	4 horas	03.06.19					
Fase 4	Integración con herramientas de monitorización	12 horas	04.06.19					

Personal: Para la ejecución de este proyecto se va a contratar un consultor senior externo. Sus honorarios son de 50 euros/hora.

. Fase 1: 6 horas (300 euros)

· Fase 2: 10 horas (500 euros)

· Fase 3: 4 horas (200 euros)

· Fase 4: 12 horas (600 euros)

Coste: En total, la ejecución del proyecto tiene un coste total para la empresa de 1600 euros

Tabla 43: Proyecto 7 - Implementación de un servicio de monitorización

Beneficios: · Identifica de manera preventiva los diversos eventos que podrían impactar sobre la continuidad de las operaciones además de su impacto económico y reputacional sobre la organización. · Minimizar o atenuar las pérdidas para el negocio en caso de desastre. . Detectar degradaciones en el servicio . Facilitar la resolución de incidencias . Centralizar los logs para mejor gestión y auditabilidad.
Riesgos a mitigar: indisponibilidad de la página web de TrendTip

Tabla 44: Proyecto 8 - Plan de Gestión del conocimiento

Plan de gestión del conocimiento
Dominio ISO: A12.Relación con proveedores, A8. Gestión de activos, A6. Organización
Objetivo: Es de interés para TrendTip retener y asegurar el conocimiento, entendiendo por conocimiento la capacidad de las personas de, en base a la información adquirida, tomar la decisión más adecuada para la organización.
Descripción: En este proyecto se ejecutará un plan de gestión del conocimiento centrado en el aprendizaje de las personas y en su desarrollo; y en la integración de su conocimiento el ciclo de negocio ayudando así a la organización a crear una estructura innovadora y eficiente que les permita alcanzar sus objetivos estratégicos.
Planificación: Para una correcta gestión del conocimiento se van a definir una serie de tareas que realizar acorde a la etapa en la que se encuentre el proyecto: Fase 1: Inicio • Identificar los procesos necesarios para conseguir que el conocimiento crítico no se escape de la organización • Identificar a los usuarios potenciales del conocimiento. • Identificar la tecnología necesaria para llevar a cabo los procesos críticos del negocio y sobre los que se sustenta la gestión del conocimiento, definiendo qué soportes y herramientas tecnológicas se necesitan. Fase 2: Ejecución: • Identificar los procesos que muestran brechas de conocimiento. • Documentar los procesos identificados acorde a los requisitos legales, contractuales y de negocio (derechos de propiedad intelectual, protección de datos, confidencialidad…). • Informar de los recursos de conocimiento disponibles a las partes interesadas relevantes y comunicar cómo estos recursos pueden usarse para abordar diferentes necesidades. Fase 3: Finalización • Documentar las lecciones aprendidas durante la realización del proyecto

Tabla 44: Proyecto 8 - Plan de Gestión del conocimiento

	Proyectos	Duración	Comienzo	Octubre				
				L	M	X	J	V
PR1	**Plan de gestión del conocimiento**	5 días	02.10.19					
Fase 1	Iniciación	1 día	02.10.19					
	Identificación procesos de negocio	3 horas	02.10.19					
	Identificación usuarios potenciales de conocimiento	3 horas	02.10.19					
	Identificación tecnología necesaria para ejecutar los procesos	2 horas	03.10.19					
Fase 2	Ejecución	3 días	03.10.19					
	Identificar los procesos que muestran brechas de conocimiento	6 horas	03.10.19					
	Documentar los procesos identificados	16 horas	03.10.19					
	Informar de los recursos de conocimiento disponibles	2 horas	05.10.19					
Fase 2	Finalización	1 día	06.10.19					
	Documentar las lecciones aprendidas	8 horas	06.10.19					

Personal: Este proyecto será ejecutado por el responsable de TI de TrendTip y será un proyecto de corto alcance

No se requiere de ningún tipo de activo adicional para la ejecución del proyecto.

Coste: Incluido dentro de las tareas del responsable de IT

Beneficios: Entre los beneficios de la gestión del conocimiento destacan los siguientes:

· Disponer de un inventario de información actualizado y disponible.

· Facilitar la transferencia de conocimiento ante bajas en el equipo.

· Conocer los procesos, proyectos y metodologías.

· Identificar brechas de conocimiento.

· Facilitar la elaboración de informes y el cálculo de KPI.

· Facilitar la transferencia de conocimiento ante cambios en el proveedor de servicios.

· Identificar la información más actualizada y completa.

Riesgos a mitigar: Indisponibilidad del servicio por la baja de un empleado o el cambio de proveedor de servicios

Anexo K: Grado de madurez controles ISO 27002 tras la ejecución de proyectos

Tabla 45: Grado madurez controles ISO 27002

ISO/IEC 27002	Control	Cumplimiento	
5	**Políticas de seguridad de la información**	**60 %**	Reproducible
5.1	Directrices de gestión de seguridad de la información	60 %	Reproducible
5.1.1	Políticas para la seguridad de la información	60 %	Reproducible
5.1.2	Revisión de las políticas de seguridad de la información	60 %	Reproducible
6	**Organización de la seguridad de la información**	**34 %**	Inicial
6.1	Organización interna	28 %	Inicial
6.1.1	Roles y reponsabilidades en seguridad de la información	80 %	Reproducible
6.1.2	Segregación de tareas	40 %	Reproducible
6.1.3	Contacto con las autoridades	0 %	Inexistente
6.1.4	Contacto con grupos de interés especial	0 %	Inexistente
6.1.5	Seguridad de la información en la gestión de proyectos	20 %	Inicial
6.2	Los dispositivos móviles y el teletrabajo	40 %	Reproducible
6.2.1	Política de dispositivos móviles	40 %	Reproducible
6.2.2	Teletrabajo	N/A	
7	**Seguridad relativa a los recursos humanos**	**51 %**	Reproducible
7.1	Antes del empleo	60 %	Reproducible
7.1.1	Investigación de antecedentes	60 %	Reproducible
7.1.2	Términos y condiciones del empleo	60 %	Reproducible
7.2	Durante el empleo	53 %	Reproducible
7.2.1	Responsabilidades de gestión	60 %	Reproducible
7.2.2	Concienciación, educación y capacitación en seguridad de la información	60 %	Reproducible
7.2.3	Proceso disciplinario	40 %	Inicial
7.3	Finalización del empleo o cambio en el puesto de trabajo	40 %	Inicial
7.3.1	Responsabilidades ante la finalización o cambio	**40 %**	Inicial

Tabla 45: Grado madurez controles ISO 27002

8	**Gestión de activos**	**36 %**	Inicial
8.1	Responsabilidad sobre los activos	40 %	Inicial
8.1.1	Inventario de activos	60 %	Reproducible
8.1.2	Propiedad de los activos	60 %	Reproducible
8.1.3	Uso aceptable de los activos	20 %	Inicial
8.1.4	Devolución de activos	20 %	Inicial
8.2	Clasificación de la información	40 %	Inicial
8.2.1	Clasificación de la información	40 %	Inicial
8.2.2	Etiquetado de la información	N/A	
8.2.3	Manipulado de la información	40 %	Inicial
8.3	Manipulación de los soportes	30 %	Inicial
8.3.1	Gestión de soportes extraíbles	N/A	
8.3.2	Eliminación de soportes	30 %	Inicial
8.3.3	Soportes físicos en tránsito	N/A	
9	**Control de acceso**	**56 %**	Reproducible
9.1	Requisitos de negocio para el control de acceso	50 %	Reproducible
9.1.1	Política de control de acceso	40 %	Inicial
9.1.2	Acceso a las redes y a los servicios de red	60 %	Reproducible
9.2	Gestión de acceso de usuario	60 %	Reproducible
9.2.1	Registro y baja de usuario	60 %	Reproducible
9.2.2	Provisión de acceso de usuario	60 %	Reproducible
9.2.3	Gestión de privilegios de acceso	60 %	Reproducible
9.2.4	Gestión de la información secreta de autenticación de usuarios	60 %	Reproducible
9.2.5	Revisión de los derechos de acceso de usuario	60 %	Reproducible
9.2.6	Retirada o reasignación de los derechos de acceso	60 %	Reproducible
9.3	Responsabilidades del usuario	60 %	Reproducible
9.3.1	Uso de la información secreta de autenticación	60 %	Reproducible
9.4	Control de acceso a sistemas y aplicaciones	52 %	Reproducible

Tabla 45: Grado madurez controles ISO 27002

9.4.1	Restricción del acceso a la información	60 %	Reproducible
9.4.2	Procedimientos seguros de inicio de sesión	60 %	Reproducible
9.4.3	Sistema de gestión de contraseñas	60 %	Reproducible
9.4.4	Uso de utilidades con privilegios del sistema	40 %	Inicial
9.4.5	Control de acceso al código fuente de los programas	40 %	Inicial
10	**Criptografía**	**80 %**	Reproducible
10.1	Controles criptográficos	80 %	Reproducible
10.1.1	Política de uso de controles criptográficos	80 %	Reproducible
10.1.2	Gestión de claves	80 %	Reproducible
11	**Seguridad física y del entorno**	**53 %**	Reproducible
11.1	Áreas seguras	60 %	Reproducible
11.1.1	Perímetro de seguridad física	60 %	Reproducible
11.1.2	Controles físicos de entrada	60 %	Reproducible
11.1.3	Seguridad de oficinas, despachos y recursos	60 %	Reproducible
11.1.4	Protección contra amenazas externas y ambientales	60 %	Reproducible
11.1.5	El trabajo en áreas seguras	60 %	Reproducible
11.1.6	Áreas de carga y descarga	N/A	
11.2	Seguridad de los equipos	46 %	Inicial
11.2.1	Emplazamiento y protección de equipos	40 %	Inicial
11.2.2	Instalaciones de suministro	40 %	Inicial
11.2.3	Seguridad del cableado	40 %	Inicial
11.2.4	Mantenimiento de los equipos	40 %	Inicial
11.2.5	Retirada de materiales propiedad de la empresa	40 %	Inicial
11.2.6	Seguridad de los equipos fuera de las instalaciones	40 %	Inicial
11.2.7	Reutilización o eliminación segura de equipos	60 %	Reproducible
11.2.8	Equipo de usuario desatendido	60 %	Reproducible
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	40 %	Inicial
12	**Seguridad de las operaciones**	**55 %**	Reproducible

Tabla 45: Grado madurez controles ISO 27002

12.1	Procedimientos y responsabilidades operacionales	27 %	Inicial
12.1.1	Documentación de procedimientos de operación	40 %	Inicial
12.1.2	Gestión de cambios	20 %	Inicial
12.1.3	Gestión de capacidades	20 %	Inicial
12.1.4	Separación de los recursos de desarrollo, prueba y operación	N/A	
12.2	Protección contra el software malicioso	60 %	Reproducible
12.2.1	Controles contra el código malicioso	60 %	Reproducible
12.3	Copias de seguridad	100 %	Optimizado
12.3.1	Copias de seguridad de la información	**100 %**	Optimizado
12.4	Registros y supervisón	40 %	Inicial
12.4.1	Registro de eventos	40 %	Inicial
12.4.2	Protección de la información de registro	40 %	Inicial
12.4.3	Registro de administración y operación	40 %	Inicial
12.4.4	Sincronización del reloj	40 %	Inicial
12.5	Control del software en explotación	60 %	Reproducible
12.5.1	Instalación de software en explotación	60 %	Reproducible
12.6	Gestión de la vulnerabilidad técnica	40 %	Inicial
12.6.1	Gestión de vulnerabilidades técnicas	40 %	Inicial
12.6.2	Restricción en la instalación de software	40 %	Inicial
12.7	Consideraciones sobre la auditoría de sistemas de información	60 %	Reproducible
12.7.1	Controles de auditoría de sistemas de información	60 %	Reproducible
13	**Seguridad de las comunicaciones**	**64 %**	Reproducible
13.1	Gestión de la seguridad de las redes	73 %	Reproducible
13.1.1	Controles de red	60 %	Reproducible
13.1.2	Seguridad de los servicios de red	60 %	Reproducible
13.1.3	Segregación de redes	100 %	Optimizado
13.2	Intercambio de información	55 %	Reproducible
13.2.1	Políticas y procedimientos de intercambio de información	60 %	Reproducible

Tabla 45: Grado madurez controles ISO 27002

13.2.2	Acuerdos de intercambio de información	60 %	Reproducible
13.2.3	Mensajería electrónica	60 %	Reproducible
13.2.4	Acuerdos de confidencialidad o no revelación	40 %	Inicial
14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**60 %**	
14.1	Requisitos de seguridad en sistemas de información	60 %	
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	N/A	
14.1.2	Asegurar a los servicios de aplicaciones en redes públicas	N/A	
14.1.3	Protección de las transacciones de servicios de aplicaciones	N/A	
14.2	Seguridad en el desarrollo y en los procesos de soporte	60 %	Reproducible
14.2.1	Política de desarrollo seguro	N/A	
14.2.2	Procedimiento de control de cambios en sistemas	N/A	
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	N/A	
14.2.4	Restricciones a los cambios en los paquetes de software	60 %	Reproducible
14.2.5	Principios de ingeniería de sistemas seguros	N/A	
14.2.6	Entorno de desarrollo seguro	N/A	
14.2.7	Externalización del desarrollo de software	60 %	Reproducible
14.2.8	Pruebas funcionales de seguridad de sistemas	N/A	
14.2.9	Pruebas de aceptación de sistemas	N/A	
14.3	Datos de prueba	N/A	
14.3.1	Protección de los datos de prueba	**N/A**	
15	**Relación con proveedores**	**60 %**	Reproducible
15.1	Seguridad en las relaciones con los proveedores	60 %	Reproducible
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	60 %	Reproducible
15.1.2	Requisitos de seguridad en contratos con terceros	60 %	Reproducible
15.1.3	Cadena de suministros de tecnología de la información y de las comunicaciones	60 %	Reproducible
15.2	Gestión de la provisión de servicios del proveedor	60 %	Reproducible

Tabla 45: Grado madurez controles ISO 27002

15.2.1	Control y revisión de la provisión de servicios del proveedor	60 %	Reproducible
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	60 %	Reproducible
16	**Gestión de incidentes de seguridad de la información**	**46 %**	Inicial
16.1	Gestión de incidentes de seguridad de la información y mejoras	46 %	Inicial
16.1.1	Responsabilidades y procedimientos	60 %	Reproducible
16.1.2	Notificación de los eventos de seguridad de la información	60 %	Reproducible
16.1.3	Notificación de puntos débiles de la seguridad	40 %	Inicial
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	40 %	Inicial
16.1.5	Respuesta a incidentes de seguridad de la información	40 %	Inicial
16.1.6	Aprendizaje de los incidentes de seguriad de la información	40 %	Inicial
16.1.7	Recopilación de evidencias	40 %	Inicial
17	**Aspectos de segruidad de la información para la gestión de la continuidad del negocio**	**87 %**	Reproducible
17.1	Continuidad de la seguridad de la información	73 %	Reproducible
17.1.1	Planificación de la continuidad de la seguridad de la información	80 %	Reproducible
17.1.2	Implementar la continuidad de la seguridad de la información	80 %	Reproducible
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	60 %	Reproducible
17.2	Redundancias	100 %	Optimizado
17.2.1	Disponibilidad de los recursos de tratamiento de la información	100 %	Optimizado
18	**Cumplimiento**	**53 %**	Reproducible
18.1	Cumplimiento de los requisitos legales y contractuales	60 %	Reproducible
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	60 %	Reproducible
18.1.2	Derechos de propiedad intelectual	60 %	Reproducible
18.1.3	Protección de los registros de la organización	60 %	Reproducible
18.1.4	Protección y privacidad de la información de carácter personal	60 %	Reproducible

Tabla 45: Grado madurez controles ISO 27002

18.1.5	Regulación de los controles criptográficos	60 %	Reproducible
18.2	Revisiones de la seguridad de la información	47 %	Inicial
18.2.1	Revisión independiente de la seguridad de la información	60 %	Reproducible
18.2.2	Cumplimiento de las políticas y normas de seguridad	20 %	Inicial
18.2.3	Comprobación del cumplimiento técnico	60 %	Reproducible

Anexo L: Informe de auditoría

Introducción

El presente documento presenta los elementos identificados en el transcurso de la acción auditora referida en el presente informe que son significativos, en tanto que se han identificado como No Conformidades (NC), Observaciones (OBS) o Puntos Fuentes (PF) en el cumplimiento de los criterios establecidos por el estándar de referencia ISO 27001:2013, y en la efectividad de dicho cumplimiento.

Objetivo

Determinar el grado de conformidad del Sistema de Gestión de Seguridad de la Información de TrendTip, en el estado vigente en la fecha de ejecución de la acción auditora, con los criterios de auditoría y evaluar su eficacia para lograr los objetivos especificados.

Alcance

El del SGSI de TrendTip, en su estado a la fecha de realización de la actividad auditora.

Definiciones

Para los propósitos del SGSI de TrendTip son de aplicación las definiciones recogidas en el documento *SGSI-Glosario de Términos* (ver sección *7. Documentación de Referencia*).

Datos Generales de la Auditoría

Horarios y Emplazamientos de la Acción Auditora

FECHA INICIO AUDITORÍA	6 de mayo de 2019
HORA DE LLEGADA	09:00
DIRECCIÓN	Oficinas TrendTip Madrid
LECTURA DEL INFORME	8 de mayo de 2019
DIRECCIÓN LECTURA	Oficinas TrendTip Madrid
HORA INICIO LECTURA	14:30
FIN DE AUDITORIA	8 de mayo de 2019

Equipo Auditor

AUDITOR JEFE SGSI

REPRESENTANTE TRENDTIP

Responsable de TI

OTROS PARTICIPANTES EN LA ACTIVIDAD

CEO

Responsable de Marketing

Responsable de ventas

ESTÁNDAR DE REFERENCIA

La auditoría se realiza frente al Estándar ISO-IEC 27002.

NOTAS SOBRE LA ACCIÓN AUDITORA

El equipo auditor informa que la presente auditoría ha sido realizada a través de un muestreo por lo que pueden existir otras no conformidades no identificadas en este informe.

Las no conformidades pueden referirse a incumplimientos de los requisitos de la norma de referencia, o de cualquier otro requisito establecido en el Sistema de Gestión de Seguridad de la Información de la Organización

Informe de Auditoría

A continuación se recogen los elementos identificados en el curso de la acción auditora, señalando las No Conformidades (NC) y las Observaciones establecidas (OBS), así como los Puntos Fuertes identificados (PF). Estos elementos se citan de acuerdo a la cláusula del estándar tomado como referencial durante la acción, y en el orden señalado.

En lo que respecta a las No Conformidades, estas se clasificarán en:

- No conformidad mayor (NC-Ma): Fallo o incapacidad de cumplir con uno o varios requisitos de la norma
- No conformidad menor (NC-Me): Error individual que levanta una duda significativa sobre la capacidad del SGSI de alcanzar sus políticas y objetivos
-

ID	Elemento Identificado	Tipo	Comentario
4. CONTEXTO DE LA ORGANIZACIÓN			
4.1 ENTENDIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha presentado el documento de contexto de la organización
4.2. ENTENDIMIENTO DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS			

		OK	Documento de alcance
4.3. DETERMINACIÓN DEL ALCANCE DEL SGSI			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha presentado el documento de alcance del SGSI
4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
			Sistema de gestión documental
5. LIDERAZGO			
5.1. LIDERAZGO E INVOLUCRACIÓN DE LA DIRECCIÓN			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha presentado la Política de seguridad firmada y aprobada, así como las actas de comités que han tenido lugar
5.2. POLÍTICA DE SEGURIDAD			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha presentado la Política de seguridad firmada y aprobada
5.3. ROLES, RESPONSABILIDADES Y AUTORIZACIONES			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha presentado convocatorias de reunión de formación y comunicación de responsabilidades para todas las personal implicadas en el alcance del sistema de gestiónades
6. PLANIFICACIÓN			
6.1. ACCIONES PARA TRATAR			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha presentado el documento de objetivos del SGSI
6.2 OBJETIVOS DE SEGURIDAD			
		ok	Durante la vista de auditoría, el Responsable del SGSI ha presentado el documento de objetivos del SGSI y se ha visto como estos se encuentran acordes a la documentación facilitada
7. APOYO			

7.1. RECURSOS			
7.2. COMPETENCIA			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha mostrado que se cuenta con un plan de formación que asegura que las personas que trabajan en TrendTip tienen las competencias necesarias para el puesto que se está desempeñando
7.3 CONCIENCIACIÓN			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha mostrado el plan de concienciación que se ha llevado a cabo
7.4 COMUNICACIÓN			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha mostrado el plan de concienciación que se ha llevado a cabo
7.5 INFORMACIÓN DOCUMENTADA			
		OK	Sistema de gestión documental
8. OPERACIÓN			
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha mostrado el análisis de riesgo ejecutado
8.2 EVALUACIÓN DE RIESGOS			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha mostrado el análisis de riesgo ejecutado
8.3 TRATAMIENTO DE RIESGOS			
		OK	Durante la vista de auditoría, el Responsable del SGSI ha mostrados los proyectos llevados a cabo a partir de los resultados del análisis de riesgo
9. EVALUACIÓN DEL RENDIMIENTO			
9.1 SEGUIMIENTO, EVALUACIÓN, ANÁLISIS Y MEDICIÓN			

		OK	Calendario de auditorías
9.2 AUDITORÍA INTERNA			
		OK	Calendario de auditorías
9.3 REVISIÓN DE LA DIRECCIÓN			
		OK	Aprobación de la dirección del plan de auditorías
10. EVALUACIÓN DEL RENDIMIENTO			
10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS			
		OK	No se dispone de informes de auditoría previos, al tratarse ésta de la primera auditoría realizada.
10.2 MEJORA CONTINUA			
		OK	La dirección es consciente de que la seguridad es un proceso continuo

ID	Elemento Identificado	Tipo	Comentario
CONTROLES ANEXO A			
A.5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			
	No hay comentarios que realizar en esta cláusula	OK	
A.6. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN			
6.1.3	Se ha detectado que no se mantiene contacto con las autoridades pertinentes La cláusula 6.1.3 establece la necesidad de mantener contactos adecuados con las autoridades competentes.	NC_MA-1	No se ha definido en todo el sistema documental cuando y a qué autoridades se deberían contactar en caso de incidente

ID	Elemento Identificado	Tipo	Comentario
6.1.4	Se ha detectado que no se mantiene contacto con los grupos de interés especial, u otros foros y asociaciones profesionales especializadas en seguridad. La cláusula 6.1.4 establece que se deben mantener los contactos apropiados con los grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	NC_MA-2	La Entidad no ha participado en ningún foro o asociación de seguridad con el objetivo de mejorar el conocimientos sobre las mejores prácticas de seguridad así como el de mantenerse actualizado con respecto a las últimas novedades.
A.7. SEGURIDAD EN GESTIÓN DE RECURSOS HUMANOS			
	No hay comentarios que realizar en esta cláusula	OK	
A.8. GESTIÓN DE ACTIVOS			
8.1.2	Los activos de la organización no cuentan con un propietario de documentando. La cláusula 8.1.2 establece que todos los activos que figuran en el inventario deben tener un propietario	NC_MA-3	En el inventario de activos mostrado, no figura el responsable de ninguno de los activos.
8.1.4	No se está evaluando que se devuelvan los activos de los empleados en caso de baja. La cláusula 8.1.4 requiere que todos los empleados y terceros deben devolver todos los activos de la organización a la terminación de su empleo, contrato o acuerdo	NC_Me -1	Una revisión de los empleados que se han dado de baja en el último año y el registro de activos de la empresa ha desvelado que el último y único trabajador en irse no ha devuelto el teléfono móvil aportado por la empresa

ID	Elemento Identificado	Tipo	Comentario
8.3.2	No se ha encontrado registro de la eliminación de soportes. La cláusula 8.3.2 establece que todos los soportes deben eliminarse de forma segura cuando no vayan a utilizarse y acorde con los procedimientos formales establecidos.	NC_Me -2	El responsable de TI ha declarado que en el último año se ha dado de baja un portátil pero que no se tiene constancia de ningún documento de baja, según consta en la normativa de gestión de activos
A.9. CONTROL DE ACCESO			
	No hay comentarios que realizar en esta cláusula	OK	
A.10. CRIPTOGRAFÍA			
	No hay comentarios que realizar en esta cláusula	OK	
A.11. SEGURIDAD FÍSICA Y DEL ENTORNO			
11.2.9	No se está siguiendo la política de escritorio despejado documentada en la normativa. La cláusula 11.2.9 establece que se adoptará una política de escritorio limpio de papeles y soportes de almacenamiento y una política de pantalla limpia para la instalaciones de procesamiento de la información	NC_Me -3	Se observó que en las oficinas de TrendTip, únicamente el responsable de TI está siguiendo la política de escritorio limpio documentada. En el resto de puestos de trabajo se encontraron papeles de carácter confidencial como la lista de empleados con sus respectivos sueldos
A.12. SEGURIDAD EN OPERACIONES TI			

ID	Elemento Identificado	Tipo	Comentario
12.6.1	El procedimiento que se está aplicando para la gestión de vulnerabilidades no se corresponde con la operativa que se está ejecutando efectivamente. La cláusula 12.6.1 establece que se debe definir las funciones y responsabilidades asociadas con la gestión de vulnerabilidades técnicas	NC_Me-4	Varias de las tareas que, según el procedimiento de gestión de vulnerabilidades debe hacer el responsable del SGSI, están siendo ejecutadas por proveedores vía contrato de servicios, reservándose el responsable del SGSI las funciones de gestión y supervisión del proceso y sus resultados. Esta discrepancia entre operativa y procedimiento debería ser solucionada.
12.6.1	Gestión unificada de vulnerabilidades para las detectadas de forma automática y de forma manual vía Hacking ético. La cláusula 12.6.1 establece que se debe definir una escala temporal para reaccionar a las vulnerabilidades encontradas	NC_Me -5	En el procedimiento de gestión de vulnerabilidades incluye en su programación la detección de las mismas tanto por métodos automatizados como mediante hacking ético, en frecuencias distintas para cada uno de los métodos. Una vez detectadas las vulnerabilidades, todas ellas son gestionadas de forma unificada (plazos de corrección, inclusión en listas de seguimientos, …) independientemente del método de detección usado.
A.13. SEGURIDAD EN LAS COMUNICACIONES			
	No hay comentarios que realizar en esta cláusula	OK	
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.			
	No hay comentarios que realizar en esta cláusula	OK	
A.15. RELACIÓN CON PROVEEDORES			

ID	Elemento Identificado	Tipo	Comentario
	No hay comentarios que realizar en esta cláusula	OK	
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
16.1.5	Efectividad en la gestión de incidentes de seguridad La cláusula 16.1.5 establece que los incidentes de seguridad de la información deben ser respondidos acordes a los procedimientos documentados.	NC_Me -6	El volumen de incidentes tratados por el Sistema de Gestión es muy bajo (7) con respecto al número de incidentes encontrados (20). La dotación de recursos para este punto mejoraría de forma objetiva en el proceso.
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			
	No hay comentarios que realizar en esta cláusula	OK	
A.18. CUMPLIMIENTO LEGAL			
	No hay comentarios que realizar en esta cláusula	OK	

Bibliografía

[1] ISO (International Standard Organization). (2013). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Estándar de Seguridad ISO/IEC 27001.

[2] ISO (International Standard Organization). (2013). Tecnología de la Información – Técnicas de seguridad – Código de prácticas para la gestión de la seguridad de la información. Estándar de Seguridad ISO/IEC 27002.

[3] ISO (International Standard Organization). (2010). Information technology -- Security techniques -- Information security management system implementation guidance. Estándar de Seguridad ISO/IEC 27003.

[4] ISO (International Standard Organization). (2009). Information technology - Security techniques - Information security management – Measurement. Estándar de Seguridad ISO/IEC 27004.

[5] ISO (International Standard Organization). (2011). Information technology -- Security techniques -- Information security risk management. Estándar de Seguridad ISO/IEC 27005.

[6] ISO (International Standard Organization). (2012). Directrices para la auditoría de los sistemas de gestión. Estándar de Seguridad ISO/IEC 19011

[7] ISO (International Standard Organization). (2018). Gestión del riesgo. Directrices. Estándar de Seguridad ISO/IEC 31000.

[8] ISO (International Standard Organization). (2015). Gestión de la continuidad del negocio ISO/IEC 22301.

[9] COBIT 5.

[10] NIST Special Publication 800-53. Security and Privacy controls for Federal Informations Systems and Organizations.

[11] Bruselas. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en:

http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l14012&from=ES

[12] Guía de seguridad (CCN-STIC-805). Esquema nacional de seguridad. Política de seguridad de la información. Disponible en:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html

[13] Guía de seguridad (CCN-STIC-806). Esquema nacional de seguridad. Plan de adecuación. Disponible en:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf

[14] Guía de seguridad (CCN-STIC-803). Esquema nacional de seguridad. Valoración de los sistemas. Disponible en:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html

[15] Guía de seguridad (CCN-STIC-804). Esquema nacional de seguridad. Guía de implantación. Disponible en:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804_medidas_de_implantacion_del_ens.pdf

[16] Guía de seguridad (CCN-STIC-802). Esquema nacional de seguridad. Guía de auditoría. Disponible en:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html

[17] Manual PILAR https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/145-ccn-stic-470b-manual-de-la-herramienta-de-analisis-de-riesgos-pilar-4-3/file.html

[18] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de elementos. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

[19] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Método. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html