Universidad de Alcalá

Escuela Politécnica Superior

Máster Universitario en Dirección de Proyectos Informáticos

Trabajo Fin de Máster

Modelo de Gestión de Seguridad Informática para 4PX Iberia

Autor: **Ciwei Bao**

Septiembre 2020

Universidad de Alcalá

Escuela Politécnica Superior

Máster Universitario en Dirección de Proyectos Informáticos

Trabajo Fin de Máster

Modelo de gestión de seguridad informática en para 4PX Iberia

Autor: **Ciwei Bao**

Directora Máster: María Jesús Lapeña

Tribunal evaluador:

Presidente:

Vocal 1º:

Vocal 2º:

Calificación:_____

Alcalá de Henares a 11 de septiembre del 2020

Primero muchas gracias a mi familia que me apoyo durante estos días especiales
Gracias a los médicos que nos protegen de las enfermedades
Muchas gracias a mi directora María Jesús
que no solo me ayudó a corregir los errores técnicos sino también los errores gramaticales

Índice

Índice de tablas

Índice de figuras

Resumen. Este proyecto tiene como objetivo diseñar e implementar un modelo eficaz de la gestión del sistema informático de la empresa 4PX Iberia, que se dedica a servicios de almacenaje y distribución de productos. Primero se va a hacer un análisis de los riesgos potenciales de la empresa, luego se proponen unas medidas para evitar o reducir riesgos detectados. A continuación, se presenta la parte de implementación y evaluación del proyecto diseñado y se comentan futuras líneas de ampliación de dicho proyecto. Finalizamos con un apartado de Conclusiones.

Palabras clave: Seguridad informática (SI), SGSI, ISO/IEC 27001

Abstract. This project focuses on designing and implementing an effective model for the management of the computer system of the company 4PX Iberia, which is dedicated to services of storage and distribute products. First, it does an analysis of the potential risks of the company, then some projects are proposed to avoid or reduce detected risks. Next, is the part of implementation and evaluation of the designed projects, later it presents the future line of this project. In the end, it shows the conclusions of the project.

1. Introducción

1.1. El proyecto

1.1.1. Objetivos

- **Objetivo General**

Este trabajo fin de máster tiene como objetivo diseñar un modelo de control de la seguridad informática (SI) para conseguir un nivel de SI adecuado en la empresa 4PX Iberia y planificar los pasos para la implementación del sistema diseñado de la gestión de SI.

- **Objetivos Específicos**

Identificar las vulnerabilidades más peligrosas de seguridad informática de empresas de servicios de envíos.

Planificar un modelo adecuado y eficaz de sistema de gestión de seguridad informática (SGSI) para compañías en dicho campo.

Buscar reglas de evaluación del SGSI aplicado.

1.1.2. Alcance

Este proyecto diseña un SGSI dirigido a controlar la seguridad informática de compañías en servicios de envíos exprés. Después de analizar las amenazas informáticas, verificamos las medidas de gestión de seguridad informática en dicha organización. Así podemos diseñar un modelo de SGSI eficaz y adecuado para estas compañías y podremos planificar cómo vamos a implementar estos controles en el futuro.

1.1.3. Ámbito

El ámbito del proyecto es el sistema informático de la empresa 4PX Iberia: los activos informáticos, sus procesos de producción, su relación con los proveedores y sus medidas actuales de control de SI.

1.1.4. Estructura del TFM

El trabajo lo estructuramos de la siguiente manera:

Empezamos con un capítulo de introducción en el que, en primer lugar; definimos en qué va a consistir este proyecto y, a continuación, presentamos y describimos el contexto donde tendrá lugar su aplicación, la empresa 4PX Iberia.

En el capítulo 2, mostramos las herramientas aplicadas en el proyecto.

En el capítulo 3, analizamos el estado actual de la SI en 4PX Iberia, listando los riesgos y las vulnerabilidades del sistema informático de la empresa.

En el capítulo 4, proponemos un SGSI para controlar el nivel de la SI en dicha empresa.

En el capítulo 5, establecemos medidas para evaluar el rendimiento del proyecto diseñado.

En el capítulo 6, mostramos los resultados del proyecto.

En el capítulo 7, comentamos las futuras líneas del proyecto.

En el último capítulo, presentamos las conclusiones del proyecto.

1.2. La empresa 4PX

1.2.1. Presentación de la empresa

Ahora los chinos hacemos compras más que nunca por Internet. Ventas por Internet han sido una parte muy importante de la economía china; además la mayoría de las ventas por Internet son productos materiales, o sea,

que los productos comprados por Internet tienen que llegar a los clientes a través de envío exprés. Un reporte de la economía china [1] demostró que la escala de ventas por Internet en China del año 2019 era más de 723,000,000,000 de dólares. Según lo publicó la Oficina Estatal de Correos de China, el año 2019 el mercado del envío exprés en China creció más de un 20% respecto al año anterior; los chinos tuvimos 63,000,000,000 de envíos y los ingresos comerciales ascendieron a unos 106,800,000,000 de dólares[2].

Creada en 2004, 4PX enfoca su negocio de gestión de envíos internacionales. 4PX es una empresa de logística muy típica en China; sus actividades de negocio, su plataforma de operación y su estructura se repiten igualmente en la mayoría de las compañías del mismo negocio. 4PX tiene su empresa matriz en Shenzhen, en el sur de China; allí tiene una oficina central con más de 5,000 empleados, Tramita unos 2 millones de pedidos diarios y consigue ventas de más de 500,000,000 de dólares al año. Con el objetivo de mejorar la calidad y la eficiencia del servicio, 4PX aplica herramientas informáticas en todas las partes de la compañía. En su oficina central, 4PX tiene un departamento de más de 200 personas para desarrollar y mantener sistemas informáticos.

4PX tiene empresas subsidiarias en 13 países y regiones por todo el mundo. En España, hay 4PX Iberia GRID S.L. (a continuación, le llamamos **4PX Iberia**); 4PX Iberia colabora con empresas como Operinter y Casesa para realizar importación y exportación, coopera con compañías como CORREOS y SEUR para enviar paquetes a sus clientes. Los servicios de 4PX Iberia son, fundamentalmente, de tres tipos: WMS, LYT y GRS.

- **WMS**—almacenamiento y distribución de productos locales; 4PX Iberia guarda los productos de sus clientes en su almacén local para ofrecer una gestión rápida y eficaz de los paquetes.
- **LYT—**paquetes pequeños internacionales; desde los almacenes chinos envían directamente a los proveedores locales del país de consignatarios. Por ejemplo, desde Shenzhen 4PX envía contenedores de paquetes pequeños al grupo CORREOS de España, luego CORREOS lleva los paquetes a los compradores. Lo que hacen en 4PX Iberia es recibir devoluciones de LYT y realizar tratamientos de devoluciones.
- **GRS—**gestión global de devoluciones; 4PX Iberia recibe devoluciones de compradores y trata las devoluciones según las comandas del vendedor.

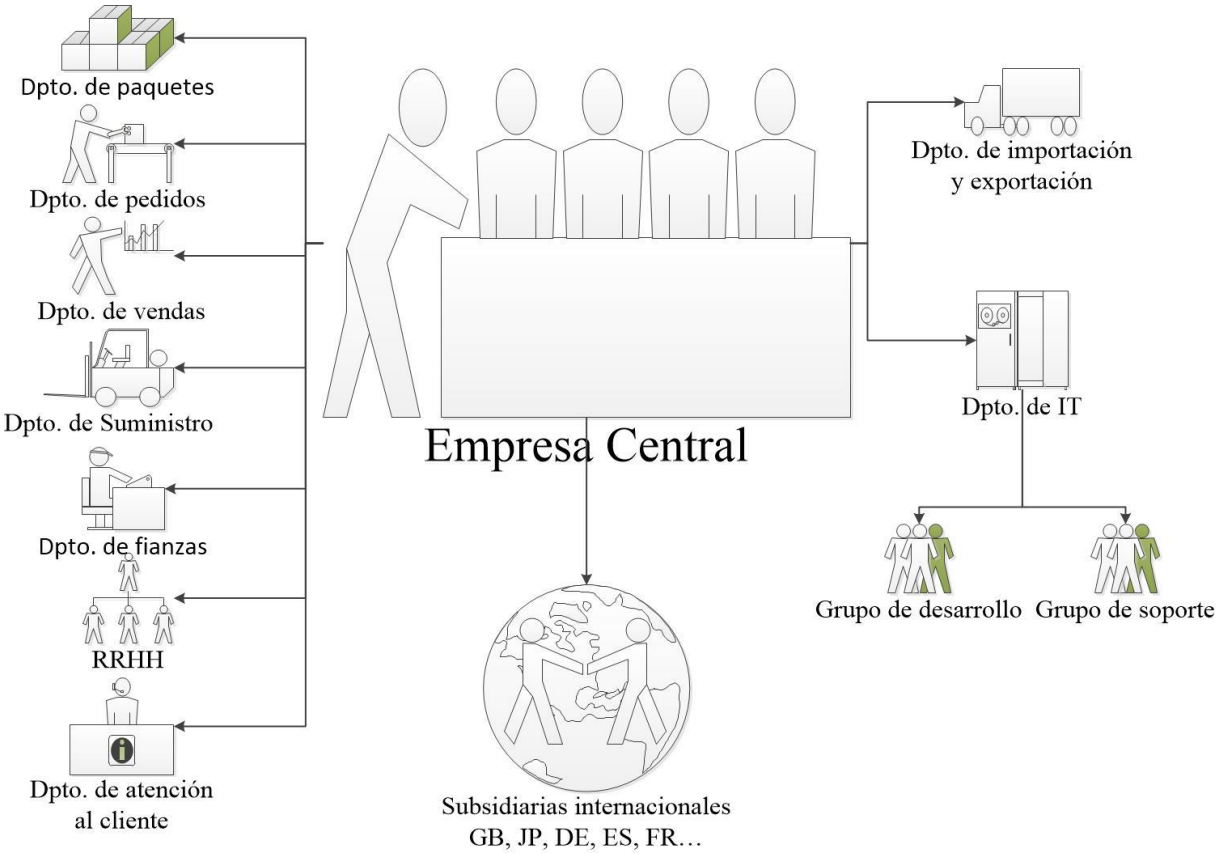
1.2.2. Estructura de la empresa

La figura siguiente represente la estructura de la empresa 4PX

[1] China B2C E-commerce Report 2019 https://www.asendia.com/asendia-insights/china-b2c-e-commerce-report-2019/

[2] China's express delivery sector registers robust growth in 2019 http://www.xinhuanet.com/english/2020-01/06/c_138682246.htm

Fig.1. Estructura de la empresa 4PX central



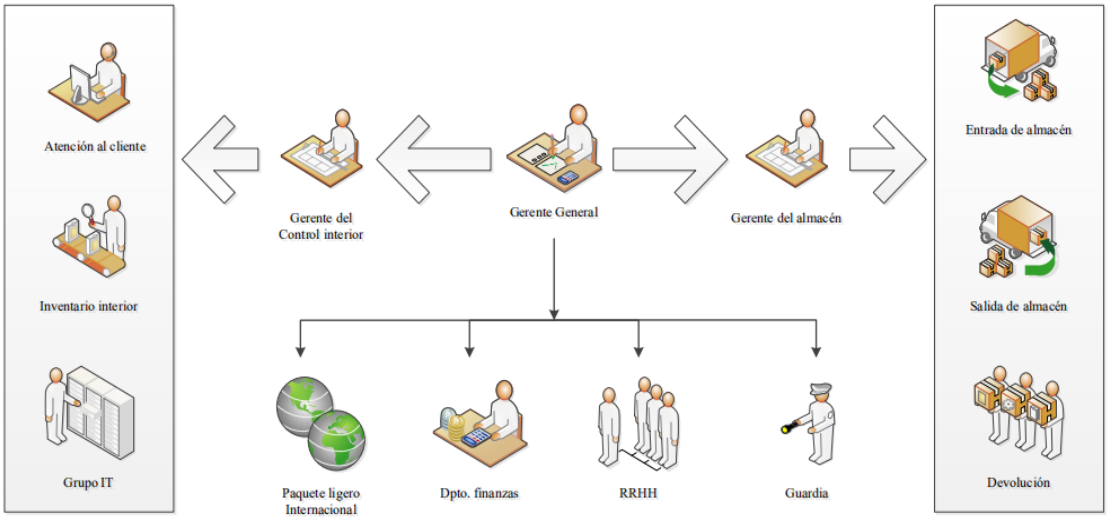
Fuente: elaboración propia

La empresa matriz 4PX mantiene un control central de toda la empresa; define los servicios en subsidiarias en diferentes países y programa aplicaciones para los procesos de producción. Las subsidirarias tienen características similares; aunque hay unas subsidiarias muy grandes, este proyecto se enfoca en las subsidiaras medianas (FR, ES, JP) para buscar un modelo adecuado del control de la seguridad informática.

- **La empresa 4PX Iberia**

La estructura de la empresa 4PX Iberia presenta el modelo de negocio de las subsidiaras de su empresa matriz. Esta figura muestra los departamentos de la empresa 4PX Iberia:

Fig.2. Estructura de la empresa 4PX Iberia



Fuente: elaboración propia

En la empresa 4PX Iberia, el gerente general administra toda la empresa; hay dos partes principales de la organización: la gestión del almacén y el control interior. La gestión del almacén controla las entradas y las salidas de productos, también se encarga los tratamientos de devoluciones; el control interior tiene tres cargas: atención al cliente, inventario interior y el grupo informático. Esta empresa tiene otros pequeños departamentos: departamento de paquetes ligeros internacionales, departamento de finanzas, departamentos de recursos humanos y guardia de seguridad.

1.2.3. Infraestructuras informáticas de 4PX Iberia

En 4PX Iberia, las infraestructuras informáticas constan de 4 partes principales: Red, ordenadores y complementos, dispositivos móviles y software. A continuación, los contenidos de cada parte.

- **Red**

  Router, Swicth, teléfono, Intranet, Internet, Wifi, Aps para ampliar el Wifi.

- **Ordenadores y complementos**

  Equipos de oficinas, equipos de operación, portátiles, impresoras, herramientas para escanear barra de códigos de productos, sistema operativo Windows 10

- **Dispositivos móviles**

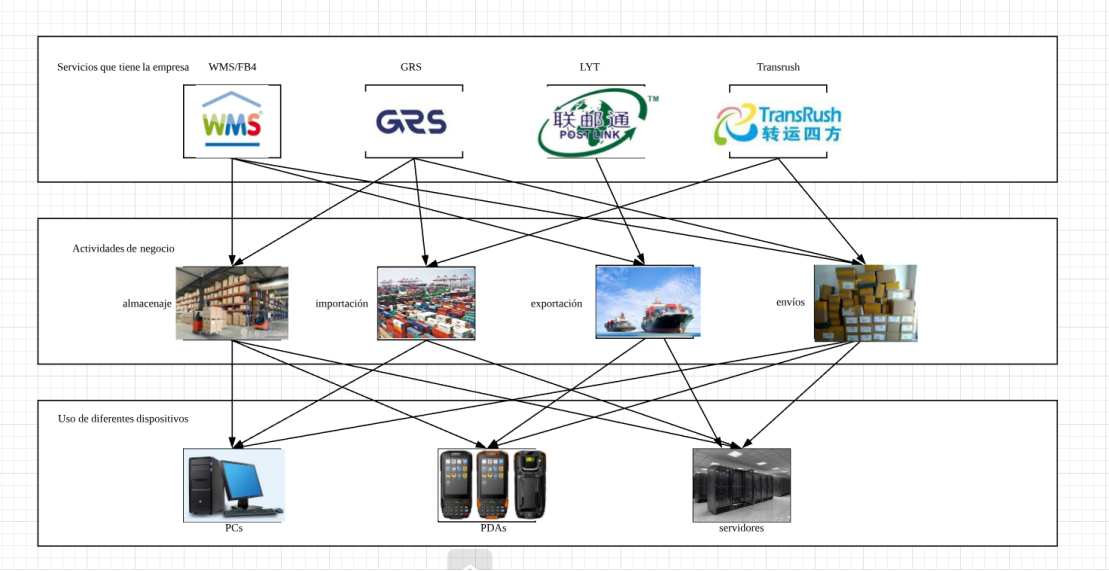
  PDAs (terminales móviles)

- **Software**

  Office, navegaciones de web, software de identificación, software de comunicación y correos

1.2.4. Mapa de activos de 4PX Iberia

Fig.3. Mapa de activos de 4PX Iberia



Fuente: elaboración propia

En el nivel básico, los activos de la empresa son: la base de datos y el servidor en la nube, copias de seguridad, documentos digitales, registración de operaciones en el sistema, software Office; PDA de operación, Router y Switch de Red, computadores etc.

En el nivel de actividades de negocio de la empresa, los activos son: recursos físicos en el almacén, compañías colaboradas de importación y exportación y paquetes de envíos.

En el nivel de servicios de la empresa, los activos son: aplicación de gestión de almacenaje, aplicación de gestión de devolución, pedidos de paquetes ligeros internacionales y pedidos de exportación.

2. Metodología

En este apartado, primero explicamos someramente los conceptos clave del proyecto, luego explicamos qué metodología seguimos en este diseño de proyecto y por qué basamos el proyecto en estas normas.

2.1. Conceptos Clave

- **Seguridad informática**

La seguridad informática se basa en un conjunto de políticas, estrategias, herramientas y procedimientos destinados a garantizar la **disponibilidad**, **confidencialidad** e **integridad** del sistema informático. El objetivo es proteger el software, hardware, redes de computadores e información evitando además fraudes, robos y daños.

- **SGSI**

Es el sistema de la Gestión de Seguridad de la Información (SGSI). Es un conjunto de las medidas de la gestión de la seguridad informática de una organización; basado en el análisis de riesgos, establece políticas y controles de la seguridad informática, define procesos de implantación, monitorización, evaluación, mantenimiento y cambios de mejora del sistema, determina la responsabilidad de la gestión de la seguridad informática en la organización.

Este sistema debe incluir estos campos: estructura de la organización de la gestión de SI, directrices y políticas de SI, objetivo y alcance del control, lista de activos informáticos, planificación de controles, procesos de la implementación, lista de verificación y métodos de mejora continua del sistema. Este sistema garantiza el desarrollo de una organización y ayuda a evitar potenciales riesgos de la información.

- **Gestión de riesgos de la información**

La gestión de riesgos de la información busca una garantía de la confidencialidad, integridad y disponibilidad del sistema informático de una organización. Podemos aplicar esta gestión de riesgos en una organización entera o en un departamento solo; pero para asegurar los rendimientos esperados, siempre repetimos los procesos de la gestión.

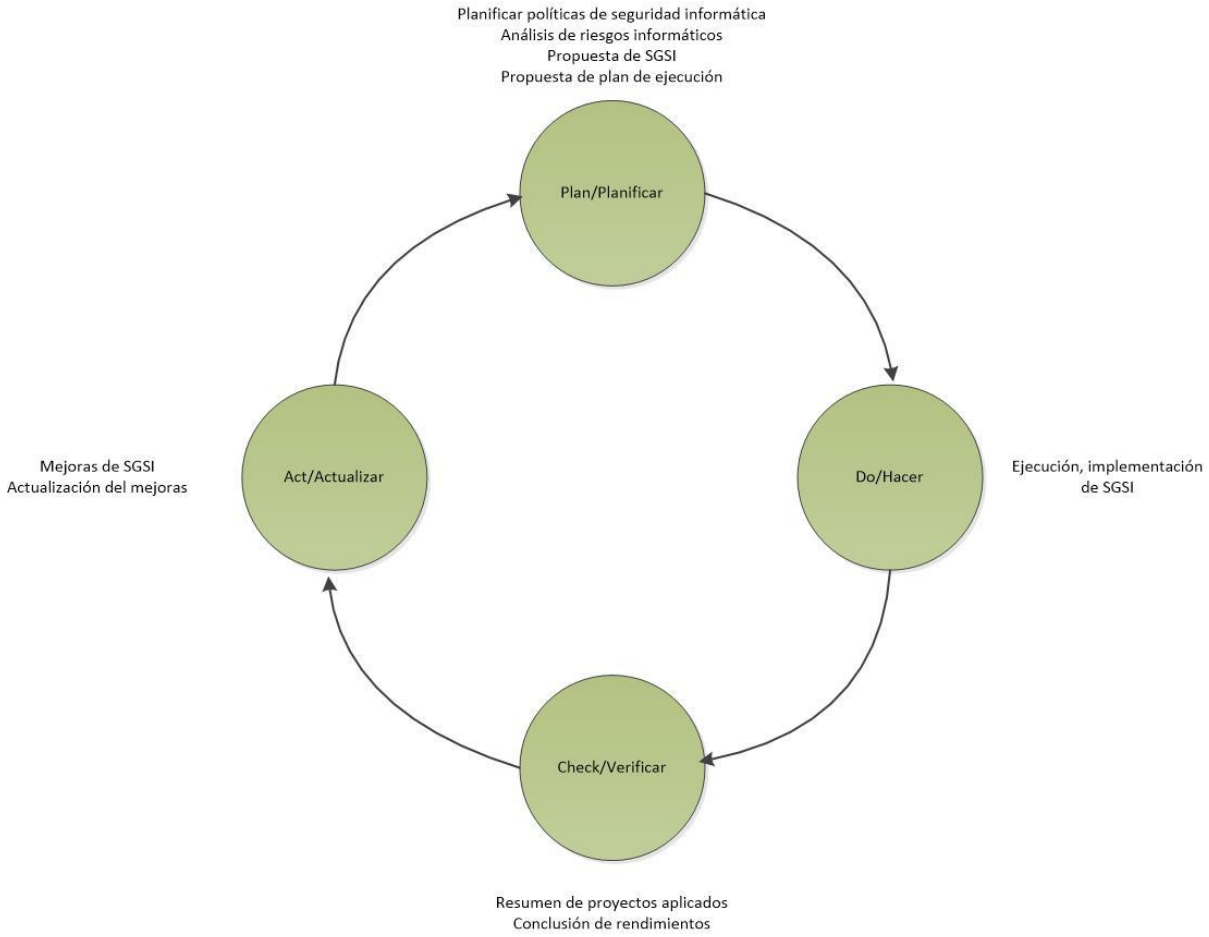
Los procesos de un círculo de la gestión son: establecimiento del alcance de la seguridad informática, análisis y evaluación de riesgos informáticos, propuesta de tratamientos, implementación y verificación de proyectos, actualización de mejora de tratamientos.

Cuando hacemos la gestión de riesgos de la información, hay que tener en cuenta que no hay seguridad absoluta, pero a través de unas estrategias adecuadas, podemos minimizar la probabilidad de riesgos y reducir sus impactos a un nivel aceptable.

- **Círculo de PDCA**

El círculo PDCA es una estrategia basada en la mejora continua de calidad. Un SGSI conta de círculos de análisis y tratamientos de riesgos; para garantizar la calidad del trabajo, siempre repite estos procesos: **Plan, Do, Check y Act.**

Fig.4. El círculo PDCA



Fuente: elaboración propia en base a ISO 27001

Plan: planificar

Definir el alcance del trabajo, identificar sus objetivos, desarrollar estrategias de SGSI y diseñar procesos para lograr los resultados esperados.

Do: hacer

Implementar controles diseñados, observar las eficiencias del trabajo realizado, apuntar los rendimientos y errores para el siguiente paso.

Check: verificar

Resumir lo resultados del proyecto, evaluar los éxitos y errores, saber las razones de la parte que se ha hecho bien, archivar la parte buenas del plan, encontrar la parte inútil y los errores ocurridos, eliminar la parte innecesaria y corregir los errores.

Act: actuar

Con los resultados obtenidos, aplicar los cambios correctivos en el sistema y volver a poner el sistema a marcha. Guardar las practicas buenas del proyecto para ser guías del próximo trabajo, resumir los errores y evitar que se repitan los problemas. Así se completa el círculo de mejora continua para volver a empezar de nuevo.

2.2. MAGERIT V.3

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por la Comisión de Estrategia TIC. Hay seis conceptos fundamentales relacionados con esta metodología: activos, amenazas, vulnerabilidades, impacto, riesgo y salvaguardas.

Hay muchas metodologías de gestión de riesgos informáticos de una organización, pero MAGERIT es una herramienta muy directa e intuitiva. Con el análisis realizado mediante tablas y técnicas gráficas no solo podemos observar los puntos débiles de la organización, sino que también podemos cuantificar las vulnerabilidades lo cual nos ayudará a decidir cuantos esfuerzas y recursos hay que poner para minimizar y controlar los riesgos detectados.

Aplicamos esta metodología para construir el modelo de gestión de seguridad informática en la empresa 4PX Iberia, seguimos las etapas de la guía: clasificar los activos informáticos de la empresa, analizar amenazas y vulnerabilidades de la empresa, calculamos los impactos y proponemos salvaguardas.

2.3. Familia de normas ISO/IEC 27000

Tiene su origen en la BS 7799-1, es una serie de mejores prácticas para ayudar a las empresas británicas a gestionar seguridad informática. Ahora la familia ISO/IEC 27000 se ha convertido el estándar internacional más conocido en el campo de seguridad informática, fue publicado por la **International Organization for Standardization** y por la **International Electrotechnical Commission**. Es una agrupación de normas de desarrollo, nos ofrece un modelo de gestión de seguridad informática para cualquier empresa u organización.

Es una familia bastante grande, las normas más relacionadas con mi TFM son ISO 27001, ISO 27002 y ISO 27005.

2.3.1. ISO/IEC 27001

Esta guía muestra qué es un SGSI (Sistema Gestión de la Seguridad informática). Esta parte nos da una buena explicación de los requisitos de un SGSI, los procesos de SGSI y el circulo PDCA. Es una explicación detallada de los pasos para construir un SGSI, los procesos de cada parte, pasos para la evaluación y formas de mejora. Indica los requisitos para establecer un sistema de gestión de la seguridad de la información en una empresa.

Aplicamos los controles del Anexo A del ISO/IEC 27001 :2013 para evaluar el estado del control de seguridad en la empresa. Al final del proyecto, usamos estos controles para comparar los rendimientos del proyecto.

2.3.2. ISO/IEC 27002

Es una guía estándar de seguridad informática y ofrece un conjunto de buenas prácticas de seguridad informática para la selección e implementación de controles de organización. Esta norma nos ayuda a analizar los puntos débiles posibles en una organización. Ofrece un marco de implementación y ejemplos dirigidos a empresas u organizaciones que quieren aplicar este modelo internacional para ayudar a controlar su seguridad informática.

Proponemos los proyectos de gestión de riesgos informáticos en base de las prácticas de esta guía.

2.3.3. ISO/IEC 27005

Esta norma se centra en el campo de control de riesgos. Esta norma contiene muchas recomendaciones y directrices para hacer una correcta administración de riesgos en una organización. Para ello, hay que analizar la situación, planificar los pasos y realizar el plan. Estas normas pueden ayudar a establecer medidas de los riesgos para saber los rendimientos del plan realizado.

En la parte del análisis de riesgo informáticos, hemos evaluado la seguridad informática de la empresa 4PX Iberia basando en estas normas y la guía MAGERIT V.3.

2.4. CMM y CMMI

CMM es el Modelo de Madurez de Capacidad, es un modelo de evaluación de los procesos del desarrollo de una organización. Define los niveles de madurez de capacidad y ayuda a la organización a hacer planificación, programación, organización y mantenimiento. CMM es el Modelo de Madurez de Capacidad Integrado, es un modelo avanzado del CMM; es un modelo para evaluar la capacidad de desarrollo de software y mejorar los procesos de programación.

En este proyecto, usamos el CMM para evaluar el estado de los controles de ISO 27001 y aplicamos el CMMI para verificar los proyectos implantados de gestión de seguridad informática.

3. Gestión de riesgos en la empresa 4PX Iberia

Sin duda, para empezar a planificar controles de seguridad informática en una compañía, hay que saber qué riesgos existen en los procesos de dicha empresa. Un análisis de riesgos que detecta los puntos débiles, ayuda a simplificar y prevenir los riesgos informáticos, facilitando el diseño de un plan adecuado para minimizar el impacto de las amenazas.

3.1. Definición

La gestión de riesgos consta de la investigación atendiendo a los valores de los activos informáticos, las amenazas potenciales y las vulnerabilidades de la organización; también incluye una evaluación de los controles aplicados, posibilidad de incidencias y sus impactos, facilitando el objetivo de obtener un nivel adecuado de seguridad informática.

3.2. Importancia

Cada vez las compañías modernas dependen más de sus sistemas informáticos. Para una empresa internacional como 4PX, la comunicación entre diferentes departamentos, la base de datos, las aplicaciones de producción y la gestión de posventa no se pueden proceder sin servicios informáticos. Al mismo tiempo, las amenazas y los riesgos informáticos están creciendo rápidamente; por ello, para asegurar la continuidad del negocio y cumplir con los requisitos legales, un control adecuado de seguridad informática es obligado.

Es una pena que, hasta ahora, la empresa todavía ignora muchos puntos importantes y no saben qué consecuencias pueden ocurrir si alguien los aprovecha. En toda la empresa 4PX no hay un departamento especial que solo se dedique a controlar la seguridad informática. En muchas empresas chinas, solo hay defensa pasiva; en otra frase, los chinos no nos fijamos en la importancia de la seguridad informática, no solemos investigar las posibilidades de problemas de la información ni gastar recursos para prevenir riesgos; dejamos la responsabilidad y el trabajo de vigilancia a las personas que desarrollaron el programa. Por eso, cuando ocurre alguna contingencia informática, siempre causa consecuencias graves.

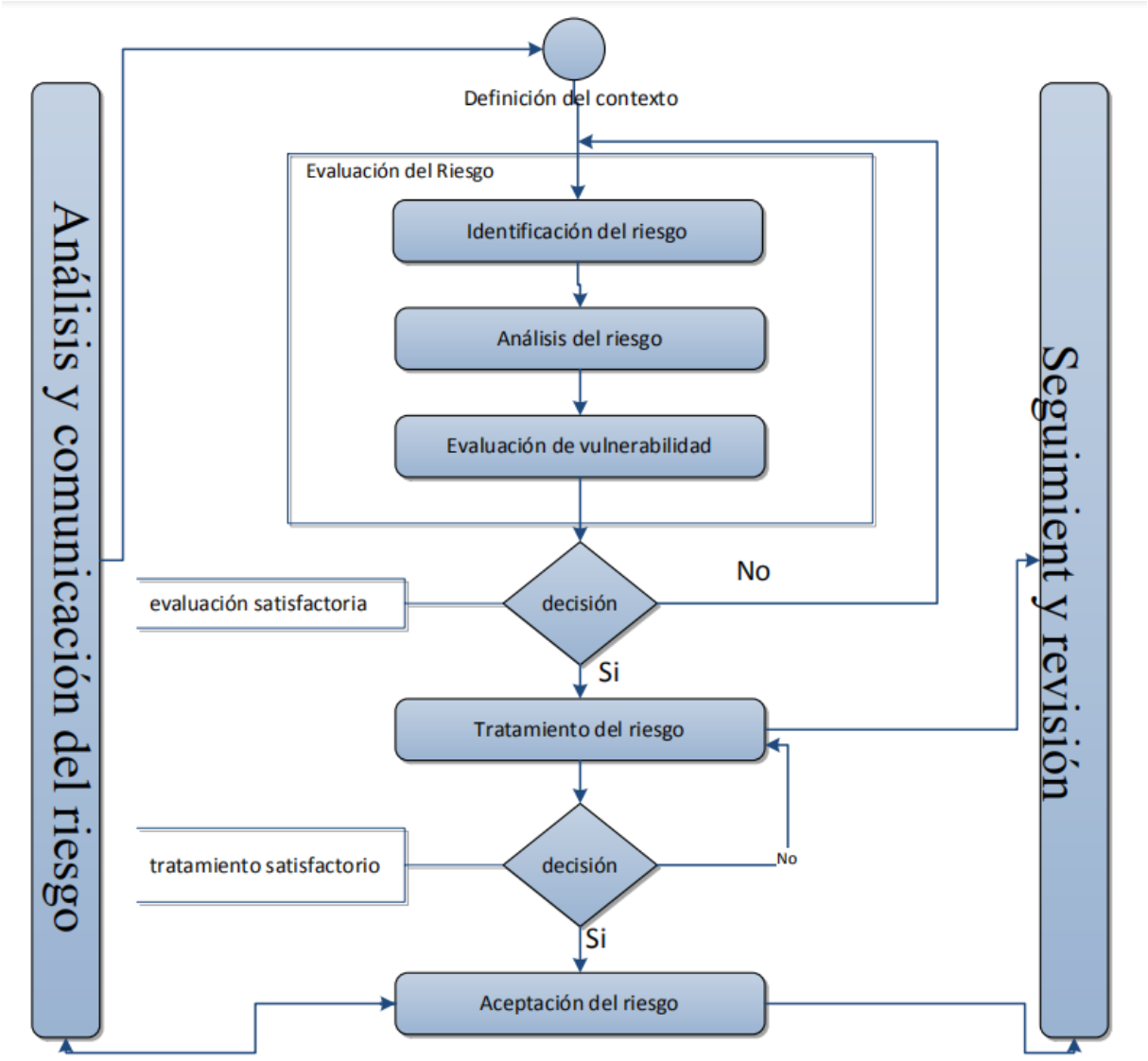
Entonces necesitamos un SGSI de calidad que garantice la seguridad de los activos; para ello, hemos de basarnos en los resultados de un análisis previo de seguridad informática, enfocando los puntos débiles, atendiendo a los costes correspondientes a los valores de los bienes informáticos. Una evaluación de seguridad informática ayuda a clarificar el estado de seguridad informática de la organización. Analizando los rendimientos de sus controles aplicados, se puede diseñar un SGSI más eficaz, más adecuado y ajustado a las necesidades específicas.

3.3. Procesos

Para realizar un análisis de riesgos informáticos riguroso y profundo, hay que seguir la estrategia de mejora continua del ciclo PDCA. El análisis de riesgos tiene estas etapas:

1. Definición del contexto: definición del alcance y de los activos informáticos.
2. Identificación del riesgo.
3. Análisis del riesgo.
4. Evaluación de las vulnerabilidades y amenazas.
5. Tratamiento del riesgo.
6. Aceptación del riesgo.
7. Comunicación del riesgo
8. Seguimiento y supervisión del tratamiento

Fig.5. Procesos de análisis de riesgos informáticos



Fuente: elaboración en base a MAGERIT V.3

3.4. Inventario de activos de 4PX

Un inventario completo de activos es la base de la gestión de riesgos informáticos, incluye información, datos, servicios, software, hardware, comunicaciones, recursos administrativos, recursos físicos y RRHH.

Tabla.1.clasificación de los activos físicos y teóricos de la empresa 4PX Iberia:

N.º de Activo	**Activos**	**Tipo**	**Descripción**
Act-001	Base de datos	Datos	Servicios de la base de datos de la empresa, conserva datos de los procesos de la compañía, documentos del sistema, reportes de trabajos realizados.

Act-002	Copias de seguridad	Datos	Copias de seguridad del servidor
Act-003	Documentos digitales	Datos	Documentos escaneados o digitales, se suelen guardar en los equipos.
Act-004	Registración de acción	Datos	Registración de operación de trabajadores, los datos están en la nube, registran entradas y salidas de trabajadores, operación de producción y solicitudes de información.
Act-005	Servidor en la nube	Servicio	Recursos de servidor en la nube, ahora 4PX no usa servidor físico
Act-006	MySQL, Java Script	Software	Softwares aplicados de la programación: la base de datos, plataformas de administración y operación.
Act-007	Office	Software	Software Office para tareas en la oficina
Act-008	Navegador	Software	Se suele usar Chrome, para entrar a las páginas de 4PX
Act-009	Control de salida y entrada	Hardware	Dispositivo inteligente de control de entradas y salidas, conoce las caras de trabajadores y registra la hora de llegada y salida.
Act-010	Router y Switch	Hardware	Router y Switch para mantener servicios de Internet, a través de ellos, más de 200 aparatos conectan con el Internet público.
Act-011	Computadores y portátiles	Hardware	Equipos con sistema operativo Window10 y básicas herramientas: Office, Chrome etc.
Act-012	Network video recorder	Hardware	Dispositivos para grabar los videos de CCTV del almacén.
Act-013	Impresora	Hardware	Dispositivo para imprimir.
Act-014	Memoria extraíble	Hardware	Incluye Pendrives y disco duros
Act-015	Internet	Comunicación	En 4PX Iberia, hay dos líneas de fibra: Movistar y Orange, el primero es para uso diario y el segundo es para urgencias.
Act-016	Intranet	Comunicación	Los equipos usan la Intranet para intercambiar datos.
Act-017	Teclados, Radones etc.	Recursos físicos	Materias de cumplimientos de computadores, para introducir y demostrar datos.
Act-018	Empleados	RRHH	Empleadores informáticos y operadores.
Act-019	Suministro de luz	Recursos físicos	Suministro estable y seguro de la luz

3.5. Análisis de amenazas

3.5.1. Requerimientos de la seguridad informática

Hay tres dimensiones básicas de la seguridad informática en una organización: disponibilidad, integridad y confidencialidad. Cuando queremos hacer una evaluación de riesgos informáticos, hay que considerar cómo afectan a cada una de ellas.

- **Disponibilidad**

Los datos del sistema y los servicios informáticos tienen que estar disponibles cuando sean requeridos. La disponibilidad asegura que el sistema no rechaza solicitudes de usuarios autorizados y da contestación a tiempo. La tabla de abajo demuestra criterios de valoración de la disponibilidad de activos en 4PX.

Tabla.2.Valoración de Disponibilidad

Puntos	Valoración	Descripción
4	Muy Alto	El valor de disponibilidad es muy alto, el uso autorizado dura 99.9% del año o no se permite interrupción del sistema. El paro de servicios causa pérdida enorme a la organización incluso penas legales.
3	Alto	El uso autorizado del sistema ocupa 90% del año; durante los procesos de producción se permite una interrupción de menos de 10 minutos.
2	Medio	El uso autorizado del sistema ocupa 70% del año; durante los procesos de producción se permite una interrupción de menos de 30 minutos.
1	Bajo	El uso autorizado del sistema ocupa 40% del año; durante los procesos de producción se permite una interrupción de menos de 1 hora.
0	No afectado	Se puede ignorar el valor de la disponibilidad, la interrupción del sistema no va a influir en la producción.

- **Integridad**

Los datos guardados y transferidos en el sistema tienen que ser correctos y completos, solo personas autorizadas pueden modificar o eliminar los datos del sistema. A continuación, se muestra la tabla con los criterios a seguir para valorar la integridad informática.

Tabla.3.Valoración de Integridad

Puntos	Valoración	Descripción
4	Muy Alto	El valor de integridad es muy alto, cambios no autorizados causan impactos graves e inaceptables, es posible parar los servicios y causar consecuencias irreparables.
3	Alto	El valor de integridad es alto, cambios no autorizados causan impactos grandes, es difícil recuperar sus consecuencias.
2	Medio	La integridad tiene valor medio, cambios no autorizados influyen en los servicios de la organización, pero es posible recuperar sus consecuencias.
1	Bajo	La integridad no tiene mucho valor, cambios no autorizados influyen un poco en los servicios de la organización, las consecuencias son fácil de recuperar.

0	No afectado	Se puede ignorar las consecuencias de cambios no autorizados del sistema.

- **Confidencialidad**

La información almacenada o transmitida solamente está alcanzada por personas permitidos, los visitantes sin autorización no tienen acceso a los datos ni pueden ver sus contenidos. La tabla abaja son los criterios de la confidencialidad.

Tabla.4.Valoración de Confidencialidad

Puntos	Valoración	Descripción
4	Muy Alto	El sistema conserva secretos más importantes; fugas de información influyen en el desarrollo de la organización. La confidencialidad influye mucho en sus intereses, la fraude o el robo de la información causa desastre a la organización.
3	Alto	El sistema conserva información reservada muy importante para la organización; fugas de dicha información causa daños graves.
2	Medio	El sistema conserva información importante de la organización; fugas de la información causa daños medios.
1	Bajo	El sistema conserva información interna de la organización, fugas de la información causa daños breves.
0	No afectado	El sistema conserva información pública de la organización; fugas de la información no afectan en nada a la organización.

3.5.2. Lista de amenazas

Previo al listado de amenazas, podemos hacer una clasificación de las mismas según sus causas. A veces los trabajadores causan pérdidas sin querer, también hay delito aprovechando vulnerabilidades de la organización. Tener en cuenta el motivo de los riesgos informáticos ayuda a proponer políticas de SI más enfocada. La tabla siguiente muestra las diferentes causas o motivos de riesgos de la información para 4PX Iberia.

Tabla.5.Motivo de incidentes

Motivo		Descripción
factores ambientales		Corte de luz, humedad o temperatura inadecuada, daños del insecto, daños de agua o fuego, desastre natural
factores personales	Intencionado	Vandalismo premeditado
		Robo interior de información
		Robo exterior de información
	involuntario	Falta de responsabilidad
		Operación prohibida, no sigue instrucciones
		Falta de formación laboral

Las principales amenazas de la empresa 4PX Iberia se muestran en la tabla de abajo.

Tabla.6.Amenazas de 4PX Iberia

N.º de amenaza	Riesgo	clasificación de amenaza
A-001	Desastres naturales	Factor natural o social
A-002	Daño de agua a equipos	error o descuido
A-003	Incendio en la oficina	gestión inadecuada de la organización
A-004	Incendio en el almacén	gestión inadecuada de la organización
A-005	Corte de luz	fallos de suministro
A-006	Corte de Internet	fallos de suministro
A-007	Atasco de servidor	fallos de software y/o hardware
A-008	Robo de contraseñas de administrador	error o descuido
A-009	Robo de contraseñas de trabajador	error o descuido
A-010	Abuso de memoria extraíble	gestión inadecuada de la organización
A-011	Abuso de dispositivo móvil	gestión inadecuada de la organización
A-012	Acceso a sistema no autorizado	abuso de autorización o acceso prohibido
A-013	Cambios no autorizados de información	ataque interno y/o externo
A-014	Fugas de la información	gestión inadecuada de la organización
A-015	Difusión de software dañino	gestión inadecuada de la organización
A-016	falsa pedido de envío	ataque interno y/o externo
A-017	robo de equipos	intrusión física y/o robo
A-018	ataque por piratas informáticas	ataque interno y/o externo

- **Pérdidas directas en caso de incidencia**

Como 4PX Iberia tiene 20 operadores en su nave y teniendo en cuenta que el coste para cada operador es 20$ por hora, podemos deducir que, cuando la emergencia para todos los equipos, la pérdida mínima es 400$/hora. En otros casos, como libre uso de dispositivos móviles o fugas de información, la pérdida es muy variable. En muchas ocasiones no pasará nada, pero a veces causa consecuencias graves incluso con penas legales. Con las valoraciones de las tres dimensiones básicas de la SI, tenemos esta tabla de valoración del impacto de cada amenaza.

Tabla.7.Valoración de impacto de amenaza

N.º de amenaza	clasificación de amenaza	Influencia en las tres dimensiones de seguridad			Suma de puntos
		Disponibilidad	Integridad	Confidencialidad	
A-001	Factor natural o social	3	0	1	4
A-002	error o descuido	2	0	0	2
A-003	gestión inadecuada de la organización	3	2	0	5
A-004	gestión inadecuada de la organización	4	0	0	4
A-005	fallos de suministro	2	0	0	2
A-006	fallos de suministro	2	0	0	2
A-007	fallos de software y/o hardware	2	0	0	2
A-008	error o descuido	2	3	3	8
A-009	error o descuido	1	0	1	2
A-010	gestión inadecuada de la organización	0	0	3	3
A-011	gestión inadecuada de la organización	0	0	2	2
A-012	abuso de autorización o acceso prohibido	0	3	3	6
A-013	ataque interno y/o externo	0	4	3	7
A-014	gestión inadecuada de la organización	0	0	4	4
A-015	gestión inadecuada de la organización	2	3	3	8
A-016	ataque interno y/o externo	0	4	0	4
A-017	intrusión física y/o robo	2	0	2	4
A-018	ataque interno y/o externo	2	3	3	8

3.5.3. Valoración de amenazas

Para valorar las amenazas informáticas consideramos dos aspectos principales: probabilidad e impacto (probabilidad de que la amenaza se materialice y daño ocasionado).

Tabla.8.Probabilidad de accidente

Puntos	posibilidad	Descripción
5	muy alto	Más de una vez a la semana, en la mayoría de los casos no es evitable.
4	alto	Más de una vez al mes, ha pasado muchas veces ya.
3	medio	Más de una vez por medio año, se puede pasar en unas ocasiones.

2	bajo	No es muy posible ocurrir, todavía no ha pasado.
1	casi imposible	Es muy imposible ocurrir, solo puede pasar en muy pocas ocasiones.

Tabla.9.Impacto de accidente

puntos	valoración	descripción
5	muy alto	El impacto es muy grave, las contingencias causan daños completos a la organización.
4	alto	Causan daños graves a la organización.
3	medio	Causan daños medios a la organización, difícil a recuperar.
2	bajo	Causan daños pequeños a la organización, fácil a recuperar.
1	muy bajo	Casi no causa daño a la organización.

Según las valoraciones de la probabilidad y el impacto, calculamos el valor de las amenazas así:

Valor de amenaza = Probabilidad * Impacto

Clasificamos los valores en esta tabla

Tabla.10. valores de amenazas

Impacto						
5 muy alto	5 ligero	10 mediano	15 grave	20 muy grave	25 muy grave	
4 alto	4 ligero	8 mediano	12 grave	16 grave	20 muy grave	
3 medio	3 ligero	6 ligero	9 mediano	12 grave	15 grave	
2 bajo	2 ligero	4 ligero	6 ligero	8 mediano	10 mediano	
1 muy bajo	1 ligero	2 ligero	3 ligero	4 ligero	5 ligero	
	1 muy bajo	2 bajo	3 medio	4 alto	5 muy alto	Posibilidad

3.5.4. Vulnerabilidades de 4PX Iberia

Según el análisis de amenazas realizado en el **apartado 3.5.2**, deducimos las vulnerabilidades de la empresa. Para obtener un valor que nos permita cuantificar las vulnerabilidades, sumamos los puntos asociados a las amenazas:

Tabla.11. Resumen de vulnerabilidades

N.º de vulnerabilidad	Descripción	Influencia	Valor
Vul-01	Factor natural o social	4	1
Vul-02	Error o descuido trabajadores	12	3
Vul-03	fallos de software y/o hardware	2	1
Vul-04	abuso de autorización o acceso prohibido	6	2
Vul-05	ataque interno y/o externo	19	4

Vul-06	gestión inadecuada de la organización	26	5
Vul-07	intrusión física y/o robo	4	1
Vul-08	fallos de suministro	4	1

En conclusión, los valores de las vulnerabilidades de 4PX Iberia son:

Tabla.12. Valor de vulnerabilidades

N.º de vulnerabilidad	Descripción	Posibilidad	Impacto	Valoración
Vul-01	Factor natural o social	1	1	1 ligero
Vul-02	Error o descuido trabajadores	4	3	12 grave
Vul-03	fallos de software y/o hardware	4	1	4 ligero
Vul-04	abuso de autorización o acceso prohibido	2	2	4 ligero
Vul-05	ataque interno y/o externo	2	4	8 mediano
Vul-06	gestión inadecuada de la organización	4	5	20 muy grave
Vul-07	intrusión física y/o robo	1	1	1 ligero
Vul-08	fallos de suministro	4	1	4 ligero

3.5.5. Tratamientos de los riesgos

Para reducir los riesgos detectados, hay estos tratamientos básicos:

- **R: Reducción de riesgo**

Medidas aplicadas para reducir la posibilidad del riesgo, sus consecuencias o ambos de estos dos.

- **A: Asunción de riesgo**

Acuerdo de mantener el riesgo del sistema, la organización mantiene el riesgo en su sistema y está preparada para sus posibles daños.

- **T: Transferencia de riesgo**

Transferir el riesgo a otra organización segura; la empresa no tiene la capacidad de responder el riesgo detectado.

- **CP: Compartición de riesgo**

Compartición del riesgo con otras organizaciones para compartir posibles daños.

Para las 5 vulnerabilidades ligeras, se toman medidas de Reducción de riesgo, Asunción de riesgo y Transferencia de riesgo.

Para la vulnerabilidad mediana, se toma la medida de Reducción de riesgo.

Para la vulnerabilidad grave, se toma la medida de Reducción de riesgo.

Para la vulnerabilidad muy grave, se toma la medida de Reducción de riesgo.

3.6. Análisis de SI con ISO/IEC 27001

Cuando se intenta planificar y diseñar un SGSI para una organización, siempre es necesario evaluar su estado actual. Después de un análisis completo de la situación actual de dicha organización, se puede proponer un modelo más ajustado y eficaz para la gestión de seguridad informática. En el Anexo A se muestran los controles de la ISO/IEC 27001; se contempla la infraestructura de un SGSI, las políticas, el liderazgo, la gestión de activos, el proceso de operación, evaluación y mejoras continuas... En la tabla que se presenta se muestra el cumplimiento de

la empresa 4PX Iberia en lo referente a los controles correspondientes a los 14 dominios de seguridad de ISO/IEC 27001. Los niveles de madurez del SGSI respecto a cada uno de los aspectos a considerar podrán ser: inexistente, inicial, procesando, parcialmente implementado y optimizado.

- **A.5 Políticas de seguridad de la información (SI)**

Las políticas de seguridad de la información proporcionan orientación y apoyo para la gestión de la información, considerando el cumplimiento de los requerimientos del negocio y la legislación vigente. Pero en 4PX Iberia, incluso en la oficina central de China, no hay ni departamento ni políticas de control de la seguridad de la información; simplemente, el grupo de programación se encarga de solucionar incidencias posibles.

- **A.6 Organización de seguridad de SI**

Marco de gestión para iniciar y controlar la implementación y operación de SI dentro de la organización. Como se dice en el punto A.5, 4PX Iberia no tiene el grupo que se dedica a controlar la SI; para dicha empresa, el primer paso de la implementación de un SGSI es establecer las políticas y marcos de SI.

- **A.7 Seguridad de los recursos humanos**

También hay que contemplar la seguridad de los recursos humanos en la organización; los empleados tienen que tener formación suficiente para cumplir los requerimientos de las leyes y para cumplir correctamente su responsabilidad y sus roles en la gestión de la seguridad de la información. Se observa que en 4PX Iberia hay un grupo de IT que está encargado de mantener la función del sistema; sin embargo, este grupo no tiene una clasificación clara de su trabajo y tiene mucha dificultad para garantizar los intereses de seguridad informática de 4PX.

- **A.8 Gestión de activos**

Se busca una identificación de los activos de la organización y una clara definición de las responsabilidades de protección. Se observa que 4PX Iberia hace una revisión de los activos físicos cada 3 meses, pero ignora la importancia de sus activos virtuales. A veces pierde sus documentales digitales.

- **A.9 Control de acceso**

Se trata de limitar el acceso a la información y a las instalaciones de procesamiento de información; también hay que controlar el acceso al sistema y servicios. Se observa que 4PX Iberia ya ha instalado dispositivo para limitar y registrar entradas y salidas de empleadores, la oficina solo deja entrada autorizada. Para el sistema, los trabajadores solo pueden usar sus usuarios; estos usuarios solo tienen acceso a los servicios autorizados. Actualmente 4PX Iberia tiene un buen control del control de acceso.

- **A.10 Criptografía**

Asegura la confidencialidad, autenticidad y/o integridad de la información. Se observa que 4PX no usa criptografía durante los procesos de comunicación y producción. No hay control de esta parte de SI.

- **A. 11 Seguridad física y ambiental**

Previene el acceso no autorizado físico, daños a las instalaciones de procesamiento de información, evita pérdida, daño o robo de los activos y la interrupción de las operaciones de la organización. Se observa que 4PX Iberia tiene vigilancia de 24 horas, en la entrada de 4PX hay control de acceso y alarmas, tiene un buen nivel de seguridad física. Pero cada mes 4PX Iberia tiene incidencia de corte de luz o Internet, 4PX ha instalado unas baterías para casos urgentes, pero no duran mucho tiempo. La seguridad de suministro de luz y Internet es el requerimiento urgente de 4PX.

- **A.12 Seguridad en las operaciones**

La seguridad de las operaciones consiste en garantizar operaciones correctas y seguras en las instalaciones de procesamiento de información, protegiendo dichas las instalaciones de procesamiento de software dañino y hacer copias de seguridad. Se observa que 4PX Iberia tiene su servidor en la nube; su servidor tiene alto nivel de seguridad y la copia de seguridad se puede hacer rápido y fácil. Los equipos también están muy seguros físicamente porque hay CCTV por todo el almacén y vigilancia de 24 horas. Pero los trabajadores pueden instalar cualquier aplicación y usar su memoria extraíble en su equipo de trabajo; es muy posible la difusión de software dañino entre los equipos de producción.

- **A.13 Seguridad en las comunicaciones**

Hay que garantizar la seguridad de la información en redes e instalaciones; también protege la información transferida dentro de la organización o con cualquiera entidad externa. 4PX Iberia usa aplicación pública para transferir información; es una aplicación segura; si hay alguna fuga de información a causa de la aplicación, se puede solicitar compensación de la compañía ALIBABA. Pero la información en los equipos no tiene seguro, solo hay aplicación básica de antivirus, esta defensa no es suficiente.

- **A.14 Adquisición, desarrollo y mantenimiento de sistemas**

La seguridad de la información es una parte importante a considerar en el desarrollo de un software. Se observa que 4PX no ha hecho suficientes pruebas de su nuevo sistema de producción. Aunque está revisando y recuperando fallos del sistema, en su aplicación todavía es posible encontrar vulnerabilidades desconocidas.

- **A. 15 Relaciones con proveedores**

Se busca una garantía de protección de los activos de la organización que sean accesibles por proveedores y, asimismo, un nivel adecuado de seguridad en los servicios con los proveedores. En el almacén de 4PX Iberia, hay área específica para carga y descargas de proveedores; además, cuando los pedidos erróneos de un proveedor llegan a 200, va a usar otro proveedor de respaldo para continuar la producción. Por tanto, 4PX tiene buena relación con proveedores.

- **A.16 Gestión de incidentes de SI**

Se trata de garantizar un enfoque coherente y eficaz para la gestión de los incidentes de SI, incluida la comunicación de eventos y vulnerabilidades de seguridad. Se observa que 4PX tiene su plan de incidentes, pero el grupo, hay personas encargadas de contingencias, pero no han establecido estrategia de gestión de incidentes, falta de análisis de vulnerabilidad y revisión de incidentes.

- **A.17 Continuidad del negocio**

La continuidad del negocio debería estar integrada en los sistemas de gestión de seguridad de la información, para asegurar la disponibilidad de instalaciones de procesamiento de información en el caso de una catástrofe. 4PX Iberia tiene su plan de continuidad de negocio, pero, igual que hemos dicho en el punto A.16, sin estrategia estable de gestión de SI ni revisión de planes de continuidad de negocio; no podemos asegurar la eficiencia de las medidas existentes.

- **A.18 Conformidad**

Evitar penas por incumplimiento de las obligaciones legales debe ser un objetivo de la seguridad informática; hay que asegurar la implementación de las políticas y procedimientos de la organización. 4PX Iberia colabora con abogados para asegurar que sus procesos de negocio no tienen partes ilegales, pero sin una supervisión de los controles de SI, es muy difícil obtener un buen nivel de control de seguridad informática.

Tabla.13. Controles de ISO 27001 antes

N.º	Cumplimiento	Inexistente	Inicial	Definido	Procesando	Administrado	Optimizado
A5	Políticas de seguridad informática	2					
A6	Organización de la seguridad informática	5	1	1			
A7	Seguridad en el personal	6					
A8	Gestión de activos	6	3	1			
A9	Control de acceso	5	3	3	1	2	
A10	Criptografía				2		
A11	Seguridad física y del entorno	4	2	3	2	4	
A12	Seguridad de las operaciones	3	1	2	2	4	2
A13	Seguridad de las comunicaciones	1		1	1	4	
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	1		1	7	4	
A15	Relación con proveedores	1	1	1	2		
A16	Gestión de incidentes de seguridad de la información	7					

A17	Aspectos de seguridad informática para la gestión de la continuidad de negocio	1	3				
A18	Cumplimiento	4	2	2			
Resumen	Una suma de los puntos	46	16	15	17	18	2

Entonces entre los 114 controles de ISO/IEC 27001:2013, 4PX Iberia solo tiene 2 controles optimizados, pero tiene 46controles inexistentes; los resultados son inaceptables, esta empresa tiene que hacer un gran esfuerzo para garantizar su negocio en España.

4. Salvaguardas de seguridad informática

Aunque 4PX ya tiene una historia de más de 16 años, no tiene un departamento que se dedique a controlar la seguridad informática. Han aplicado algunos controles básicos en la empresa; por eso, antes de empezar a implantar un nuevo SGSI, hay que verificar los controles existentes. A través de una evaluación completa de su eficiencia, se puede proponer una nueva versión más completa y eficaz.

Después de comprobar los requerimientos de seguridad informática de 4PX y la situación actual de la seguridad informática, proponemos un nuevo SGSI. Este sistema gastará recursos aceptables y conseguirá un nivel adecuado de SI. En el futuro, este plan servirá también para solicitar certificación de ISO/IEC 27001.

4.1. Política general y liderazgo de SI

La política de seguridad de la información es la base fundamental de un SGSI para una organización; establece reglas para garantizar la confidencialidad, disponibilidad e integridad de la información. Es una buena explicación de los que queremos proteger y el porqué; por eso, hay que definir la política de una forma muy clara, hay que comunicarla a todos los miembros de la organización y hay que verificar que se cumple.

El liderazgo es otra parte fundamental del SGSI, es el motor de todos los controles de la seguridad informática. Involucrar a la alta gerencia dentro del sistema de gestión de SI asegura el apoyo desde la parte administrativa de la organización. También garantiza la coordinación de las estrategias de la organización para conseguir los objetivos de SI.

- **Objetivo**

El objetivo es establecer políticas de SI para la empresa 4PX Iberia y buscar el marco adecuado de liderazgo en dicha organización.

- **Alcance**

Las políticas establecidas son para todos los trabajadores de la empresa 4PX Iberia y todos los activos informáticos de dicha empresa.

El liderazgo incluye a todos los miembros de la empresa 4PX Iberia y alguna alta gerencia de la empresa matriz en China.

- **Soluciones**

1. Con el fin de arrancar el proyecto de proteger la seguridad de la información, debe establecerse el liderazgo y el grupo de la gestión de la seguridad de la información; para 4PX, se propone un director de la seguridad informática para las subsidiarias en Europa. En 4PX Iberia, definen el grupo de IT que también se encarga de la gestión de seguridad informática, y consta de un jefe y dos miembros.
2. Establecer estrategias de la gestión de seguridad de la información según los servicios de 4PX Iberia y considerando leyes de España y Europa.
3. Evaluar el entorno de riesgos de seguridad informática en 4PX Iberia.
4. Publicar una declaración del objetivo y principios de la gestión de SI.
5. Identificar la segregación de roles de administración y responsabilidad (organigrama de responsabilidades).
6. Las políticas principales son: control de acceso del sistema, identificación de la información y su tratamiento, normas de dispositivo móvil, seguridad física, seguridad de comunicación y defensa de software dañino.
7. Proponer gestión de cambios de la política de SI; cuando hay cambios grandes, hay que solicitar permiso del director. Los cambios tienen que coordinar las estrategias de gestión de la SI en toda la empresa.

4.2. Normas de uso de activos informáticos

- **Objetivo**

Establecer normas correctas del uso de activos informáticos de la empresa, estrategias de tratamiento de la información y segregación de uso de equipos

- **Alcance**

Activos informáticos de 4PX Iberia, la información de producción, equipos de trabajo

- **Solución**

Gestión de activos informáticos de 4PX Iberia

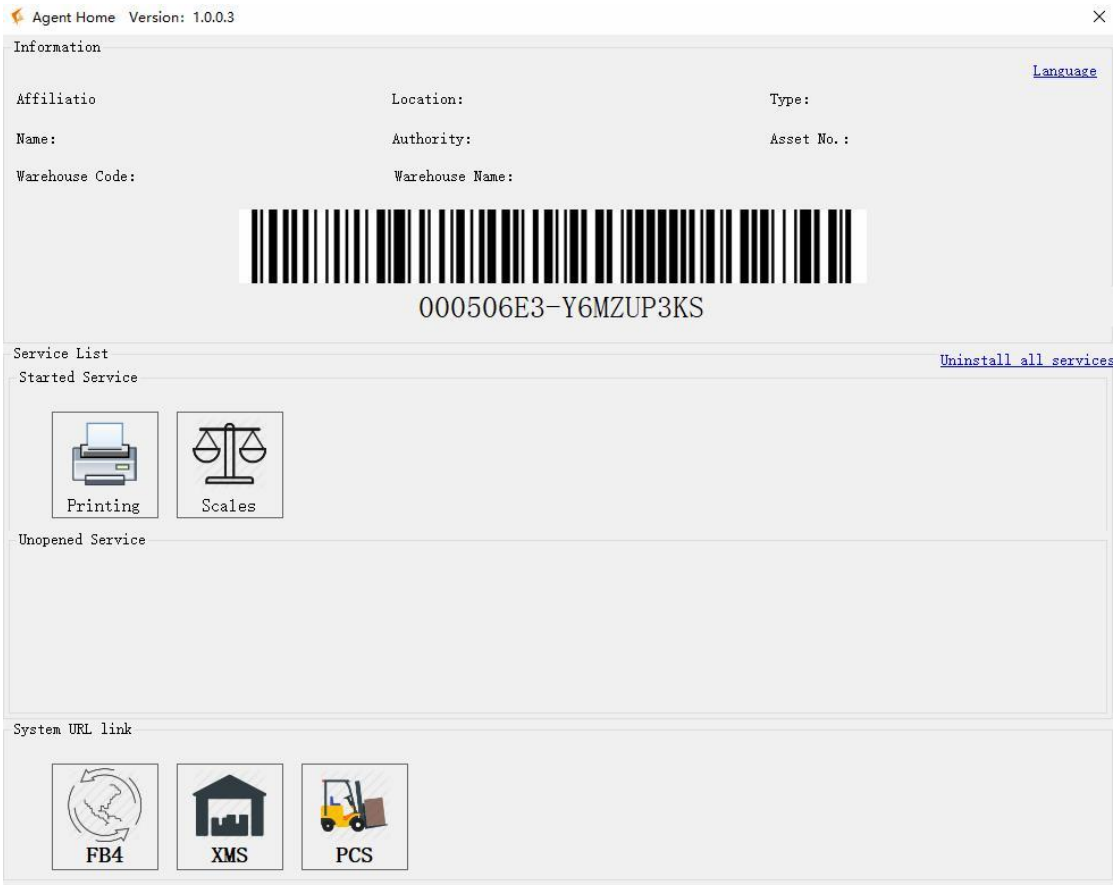
Tras el análisis de riesgos de la información, se observa que, en 4PX Iberia, solo hay un control de los activos físicos, pero falta una gestión completa de los otros tipos de activos de 4PX Iberia. El objetivo de este proyecto es completar la parte que falta y mejorar el control existente de activos físicos en la empresa. Las tareas concretas a realizar son:

1. Identificar los activos informáticos y revisar el ciclo de vida de la información, que incluye estas etapas: creación, tratamiento, almacenaje, transferencia, eliminación y destrucción.
2. Definir el uso responsable de la información; una vez se autoriza a una persona o a un grupo a usar unos activos informáticos, hay que definir la responsabilidad de protección de los activos y revisar periódicamente los accesos y operaciones de personas autorizadas.
3. Una vez la persona autorizada termina su trabajo en la organización, tiene que devolver los activos autorizados; la empresa también tiene que dar por finalizado su permiso de acceso a la información de la empresa.
4. Identificar la información importante de la empresa, decidir estrategias de tratamientos de la información; por ejemplo, para información de datos de los destinatarios de paquetes, solo se puede copiar con un pendrive concreto y hay que marcar señal llamativa en el pendrive.
5. La memoria extraíble tiene que ser rastreable, bien guardada, cifrada y registrada.
6. Para destruir la memoria extraíble, hay que formatearla y destruirla físicamente.

Aplicación de autorización y segregación de equipo

Para identificar los equipos que conectan al centro de base y limitar el acceso de computadores desconocidos, 4PX ha diseñado una aplicación que se llama AGENT. Una vez está instalado esta aplicación en los computadores, se va a crear un código único; pueden añadir estos códigos en la página de administración para autorizar estos equipos. Cuando han distribuido autorizaciones de los equipos, los trabajadores ya pueden empezar a hacer su trabajo en los equipos autorizados.

Fig.6. La aplicación Agent



Fuente: captura de pantalla de la aplicación

La figura arriba es una captura de la aplicación AGENT. Este equipo tiene su propio código único. Como se ve en la imagen, este equipo tiene autorizaciones a imprimir etiquetas y pesar productos.

4.3. Normas de usuario y contraseña

- **Objetivo**

  Establecer uso correcto de usuarios y contraseñas

- **Alcance**

  Usuarios de acceso y contraseñas

- **Solución**

La empresa 4PX Iberia obliga a todos sus empleadores a utilizar un usuario único; el gerente general del almacén local distribuye autorización de cada usuario. Cuando el trabajador entra al sistema con su usuario, solo puede ver la parte del sistema que tiene el permiso de acceso.

Usuario

1. Una vez un trabajador nuevo empieza a trabajar en 4PX Iberia, le dan una cuenta única. En esta cuenta introducen su información básica: nombre, sexo, teléfono y cargos en la empresa.
2. El sistema registra todas las actividades de los usuarios, para los envíos que salen del almacén de 4PX Iberia, se puede hacer un seguimiento completo; desde que se recoge de la estantería hasta que se mete al contendor de los proveedores, el operador de cada proceso está registrado.

3. Cuando el empleado de 4PX Iberia termina su trabajo, tiene que cerrar su sesión y dejar el escritorio limpio. Cuando tiene que interrumpir su trabajo, también tiene que cerrar su sesión del sistema, si no lo hace y alguien aprovecha el hueco de su ausente, este empleador también tiene las culpas de los errores.
4. Para usar PDA los operadores tienen que entrar con su usuario, el administrador distribuye tareas a su cuenta, solo pueden ver sus tareas propias. La aplicación de 4PX en la PDA no puede memorizar contraseñas y cuando terminan su jornada del día, tienen que cerrar la sesión. Para el caso de olvido, la sesión de la PDA termina en 20 minutos si no hay operaciones.

Contraseña

1. El empleado debe cambiar su contraseña en su primer ingreso.
2. Tiene que usar contraseña difícil a adivinar, que tiene 8 caracteres, una letra minúscula, una letra mayúscula, un carácter especial y un número.
3. Están prohibido el uso de nombre o cumpleaños como contraseña, el uso de letras continuas en teclado también está prohibido.
4. Se obliga a cambiar contraseña en 45 días naturales.
5. No se puede usar contraseñas iguales, la contraseña no se puede repetir dentro de un año.
6. No se puede apuntar la contraseña cerca de la mesa de operación, tiene que memorizar la contraseña.

4.4. Normas de dispositivos móviles

- **Objetivo**

Establecer normas de uso de dispositivos móviles para el lugar de producción y las oficinas de 4PX Iberia.

- **Alcance**

Todos los operadores del almacén y empleadores de las oficinas, todos los dispositivos móviles incluso móviles personales y PDA (terminal móvil de operación) de la empresa.

- **Solución**

Móviles personales

Prohíben a todos los operadores la entrada con sus móviles personales; en la entrada del almacén han dejado una taquilla electrónica para guardar todas las cosas personales. Detrás del control de entradas, hay una puerta de inducción de metal; solo personas autorizadas pueden entrar con sus móviles. La secretaría de la oficina contesta llamada externas y en caso de emergencia, los operadores pueden usar el teléfono fijo para comunicar con su familia.

PDA

Para PDA (terminal móvil de operación) del almacén, hay un control muy estricto:

1. Cada empleado tiene su PDA correspondiente, el código IMEI está apuntado en un fichero para casos de pérdidas.
2. En la PDA está instalado la aplicación para localizar el dispositivo, en caso de pérdida, si todavía está en la nave y tiene conexión a Internet, se puede encontrar la PDA.
3. El empleado solo tiene permiso limitado de la PDA, no tiene contraseñas para descargar aplicaciones, cuando recibe la PDA, ya tiene las aplicaciones necesarias para trabajar.

4.5. Control de acceso y seguridad física

- **Objetivo**

Establecer estrategias de protección de seguridad física de la empresa, aplicar tecnologías modernas para garantizar la seguridad física de las oficinas y del almacén.

- **Alcance**

Control de entrada y salida, CCTV, activos físicos de la empresa.

- **Solución**

Control de entrada y salida

4PX Iberia ha instalado un control inteligente de ZKTECO, pueden introducir datos básicos de los empleados y escanear sus caras. Cuando los empleados entran y salen, el sistema registra todos estos movimientos y calcula la hora de trabajo. Atrás del control hay una puerta con sensor de metal.

La persona encargada de analizar las horas de trabajo descarga los datos del día anterior y verifica si cumplen las horas del trabajo y comprueba si hay entrada o salida rara.

En 4PX Iberia hay una buena segregación de espacio, los trabajadores tienen que introducir su código personal para abrir la puerta de separación. Cuando una persona quiere entrar a un lugar no autorizado, su código no va a abrir la puerta.

CCTV

4PX Iberia instala un sistema de CCTV, que consiste en más de 60 cámaras y dos grabadoras de video. Los equipos de CCTV están localizados en la oficina, la memoria es suficiente para guardar videos de un mes. El sistema tiene una opción que solo guarda video cuando hay movimientos de personas. Si aplican esta estrategia, se puede guardar video de dos meses. También es posible descargar video de un periódico de tiempo con memorias extraíbles.

Solo personas autorizadas tienen acceso a los equipos de CCTV, los equipos tienen contraseñas para realizar consultas de videos. Cada año, el proveedor de CCTV viene dos veces para revisar y hacer el mantenimiento des CCTV. La figura de abajo es el sistema de CCTV en 4PX.

Fig.7. CCTV en 4PX Iberia

Fuente: foto en la oficina de 4PX

Políticas de seguridad física

Para asegurar la seguridad física en 4PX, establecen las medidas que se indican a continuación:

1. Los accesos de visitantes están registrados, mantienen la vigilancia a los visitantes para que solo visiten los lugares autorizados.
2. No se puede consumir alimentos en la nave, ni se puede dejar botella de agua abierta cerca a los equipos. Cada mes hay que revisar los cables y los enchufes, no se permite conexión peligrosa de la luz. Se mantiene la revisión de los 30 extintores por toda la nave.
3. Al final del día, los trabajadores que usan portátiles tienen que apagar el equipo y guardarlo en su armario, cerrar el cajón con llave y llevarse su llave. Los objetos valiosos tienen que guardarse en lugar seguro; por ejemplo, antes de salir los trabajadores tienen que dejar su PDA en la oficina.
4. Al final, antes de terminar la jornada, tienen que cerrar las oficinas con llaves y poner la alarma de seguridad.
5. Hay que definir claramente la zona de intercambio, separar espacio para diferentes proveedores, asegurar la vigilancia mientras carga y descarga. Se limita el acceso del transportista, no puede visitar sitio sin autorización.
6. Cifrar los discos duros de los equipos.

4.6. Prueba y mantenimiento de aplicaciones y servidor

- **Objetivo**

Comprobar que las aplicaciones funcionan correctamente y, en su caso, detectar posibles errores

- **Alcance**

El departamento de programación de la empresa matriz de 4PX, el grupo IT de 4PX Iberia, los empleados de 4PX Iberia y las aplicaciones diseñadas

- **Solución**

El año 2019, 4PX empezó a usar su sistema nuevo; esta vez han cambiado mucho: usan el servidor en la nube a sustituir servidores locales en los almacenes extranjeros, usan páginas de web para acceder a los servicios en el lugar de programaciones de Java. Hay muchas renovaciones buenas del sistema nuevo; pero como tenía mucha prisa para arrancar el sistema nuevo, no habían hecho suficientes pruebas del sistema. Por eso, este sistema todavía tiene muchos fallos. Están arreglando los errores, pero reparar un coche marchando es más difícil que en su fábrica.

Por eso, ahora el grupo informático de 4PX Iberia va a comunicar con su empresa matriz para buscar un modelo más adecuado del diseño de aplicaciones nuevas:

1. Antes de la programación, el departamento informático de la empresa matriz tiene que confirmar la necesidad de la aplicación nueva.
2. Después de programar una aplicación nueva, tienen que contactar con el grupo de 4PX Iberia para hacer una serie de pruebas de la aplicación. Los datos de la prueba tienen que ser bien elegidos y protegidos.
3. Antes de poner en marcha la nueva aplicación, hay que comunicar con el equipo local y dejar tiempo para realizar formación a los empleados.
4. Después de la actualización de las aplicaciones, hay que mantener revisión habitual de las aplicaciones.

4.7. Formación y concienciación de operadores

- **Objetivo**

Asegurar una formación correcta y adecuada a todos los empleados de 4PX Iberia, garantizar que todo el mundo conoce las normas de control de SI.

- **Alcance**

Todos los empleados de 4PX Iberia, políticas de seguridad informática y normas de protección de SI para dicha empresa.

- **Solución**

La oficina central de 4PX prepara un documento de los detalles de los controles de seguridad informática para la organización. Este documento consiste en el objetivo de gestión de seguridad informática, las normas de controles y posibles sanciones. Esta formación tiene el apoyo de la gerencia alta de la empresa matriz, la formación de SI no es un cargo innecesario sino es una parte importante del negocio de la empresa.

Tras la formación, los trabajadores tienen que saber las operaciones prohibidas y las reglas que tienen que cumplir durante la producción. La formación de SI asegura que toda la organización tiene la misma orientación de SI, esto el objetivo fundamental de la implantación de políticas de seguridad informática.

4.8. Gestión de incidente y continuidad de negocio

- **Objetivo**

Se buscan estrategias de continuidad de negocio tras incidentes y normas adecuadas de revisión habitual

- **Solución**

Corte de luz

1. Apagar equipos para ahorrar la electricidad de la batería[3]
2. Usar portátiles para seguir la producción
3. Revisar la caja de electricidad para saber si se ha desconectado alguno saltador. Llama al técnico para solucionar el caso actual.
4. Avisar a la oficina central de los posibles retrasos en caso de largo tiempo de corte de luz
5. Analizar posteriormente de la corte de luz, detectar el origen y citar con el técnico para solucionar el problema

Corte de Internet

1. Usar la línea del Internet de respaldo para seguir la producción. Cuando hay caída de las dos líneas, compartir los datos de los móviles preparados
2. Revisar el Rúter, Switch y cables de Internet
3. Volver a encender el Internet principal
4. Llamar al técnico si no funciona las estrategias arriba
5. Analizar la cause de caída del Internet, evitar que se repita en mismo caso.

Caso de fallos de comunicación con proveedor

1. Cuando los envíos erróneos sobrepasan 200, cortar esta línea y usar otro proveedor para continuar la producción.
2. Avisar al proveedor el caso para detectar las causas
3. Solucionar problema encontrado y hacer pruebas
4. Volver a activar el proveedor parado
5. Analizar posteriormente y evitar el mismo caso en el futuro

Para dicha empresa 4PX Iberia también están preparando más planes de continuidad de negocio, por ejemplo, plan en caso de fuego, en caso de COVID-19 etc.

[3] Una batería está instalada para el caso de emergencia, pero antes no dura mucho tiempo porque tienen todos los equipos encendidos en caso de corte de luz.

5. Implementación del SGSI

5.1. Propuesta de proyectos de seguridad

Desde el mayo de 2019 hasta el mayo de 2020, la empresa 4PX Iberia ha crecido cinco veces; de 6 empleados a 30 empleado, de 600 pedidos diarios a 4000. Es muy posible que el próximo año 2021, 4PX Iberia tendrá una escala de más de 100 empleados, como otros almacenes de 4PX en Reino Unido, Alemania y República Checa.

Al mismo tiempo, ya no se puede ignorar la importancia de control de SI de la organización. Además, en julio ha ocurrido una intrusión no autorizado en el sistema de control de entradas y salidas; la causa de esta incidencia era que no habían cambiado la contraseña por defecto. Por eso, 4PX Iberia empieza a tomar medidas para obtener un nivel adecuado de seguridad informática; si los resultados satisfacen a las gerencias altas de su empresa matriz, es muy probable aplicar el modelo de 4PX Iberia a todas sus subsidiarias por todo el mundo.

Dicha empresa decide usar 7 meses para establecer un SGSI adecuado, de junio a diciembre de 2020; 4PX Iberia quiere analizar los riesgos de la información e implementar tratamientos de las amenazas. El año 2021, si los rendimientos del SGSI salen satisfactorios, se planteará la solicitud de la certificación de ISO/IEC 27001 para dicha empresa.

Los procesos de implementación de un SGSI consisten en:

1. Identificación de proyectos de SI
2. Plan de ejecución
3. Ejecución y monitorización.

Para reducir el impacto de las amenazas detectadas, el grupo de IT de 4PX Iberia propone esta lista de proyectos poniendo el énfasis en las vulnerabilidades de la organización.

Tabla.14. Proyectos de seguridad

N.º de proyecto	Nombre de proyecto	Subproyecto	Vulnerabilidad relacionada
P-01	Análisis de riesgos informáticos	Análisis de riesgos	Evaluación según ISO/IEC 27001
P-02	Política general y liderazgo de SI	Políticas de seguridad informática	Vul-06
		Liderazgo de seguridad informática	Vul-06
P-03	Normas de uso de activos informáticos	Gestión de activos Informáticos	Vul-04, Vul-05, Vul-06
		Aplicación de autorización y segregación de equipo	Vul-03, Vul-04, Vul-05
P-04	Normas de usuarios y contraseñas	Normas de usuarios	Vul-04, Vul-05, Vul-06
		Normas de contraseñas	Vul-04, Vul-05
P-05	Normas de dispositivos móviles	Normas de uso de móvil personal	Vul-02, Vul-03, Vul-05
		Normas de uso de PDA	Vul-03, Vul-07
P-06	Control de acceso y seguridad física	Control de entrada y salida	Vul-07
		CCTV	Vul-02, Vul-07
		Políticas de seguridad física	Vul-05, Vul-07
P-07	Prueba y mantenimiento de aplicaciones y servidor	Prueba y revisión de aplicaciones	Vul-03
		Copias de seguridad y mantenimiento de la base de datos	Vul-01, Vul-03, Vul-04 Vul-05

P-08	Formación y concienciación de operadores	Formación de empleados	Vul-02, Vul-04, Vul-05, Vul-06
P-09	Gestión de incidente y continuidad de negocio	Evaluar incidente posible	Vul-01, Vul-08
		Planes de emergencia	Vul-01, Vul-08
		Registración y revisión de incidente	Vul-03, Vul-05, Vul-06, Vul-08

5.2. Plan de ejecución de SGSI

Para visualizar las acciones de ejecución de los proyectos, se aplica el diagrama GANTT[4].

Tabla.15. Proyectos en detalle

N.º de proyecto	Tareas en detalle	Fecha de inicio	Fecha de fin	Duración(días)	Responsabilidad	Cumplimiento
P-01	1. Definición del contexto	1-Jun-20	7-Jun-20	7	Grupo de IT de 4PX Iberia	100%
	2. Análisis de activos informáticos	8-Jun-20	14-Jun-20	7	Grupo de IT de 4PX Iberia	50%
	3. Evaluación de riesgos informáticos	15-Jun-20	28-Jun-20	14	Grupo de IT de 4PX Iberia	50%
	4. Plan de tratamiento de riesgos	29-Jun-20	12-Jul-20	14	Grupo de IT de 4PX Iberia	25%
	5. Comunicación de riesgos	13-Jul-20	19-Jul-20	7	Grupo de IT de 4PX Iberia	50%
P-02	1. Autorización de gerencia alta y liderazgo	20-Jul-20	26-Jul-20	7	Gerente general de 4PX Iberia	100%
	2. Elaborar la política general de SI para 4PX Iberia	27-Jul-20	16-Aug-20	21	Grupo de IT de 4PX Iberia	50%
	3. Educar a sus empleados	17-Aug-20	23-Aug-20	7	Grupo de IT de 4PX Iberia	25%
	4. Monitorizar, actualizar y retirar de política de SI	24-Aug-20	31-Dec-20	130	Grupo de IT de 4PX Iberia	10%
P-03	1. Gestión de los activos informáticos	15-Jun-20	28-Jun-20	14	Grupo de IT de 4PX Iberia	25%
	2. Segregación y autorización de equipos	29-Jun-20	12-Jul-20	14	Grupo de IT de 4PX Iberia	100%
P-04	1. Usuario único para cada empleado	10-Aug-20	16-Aug-20	7	Director de RRHH de 4PX Iberia	100%

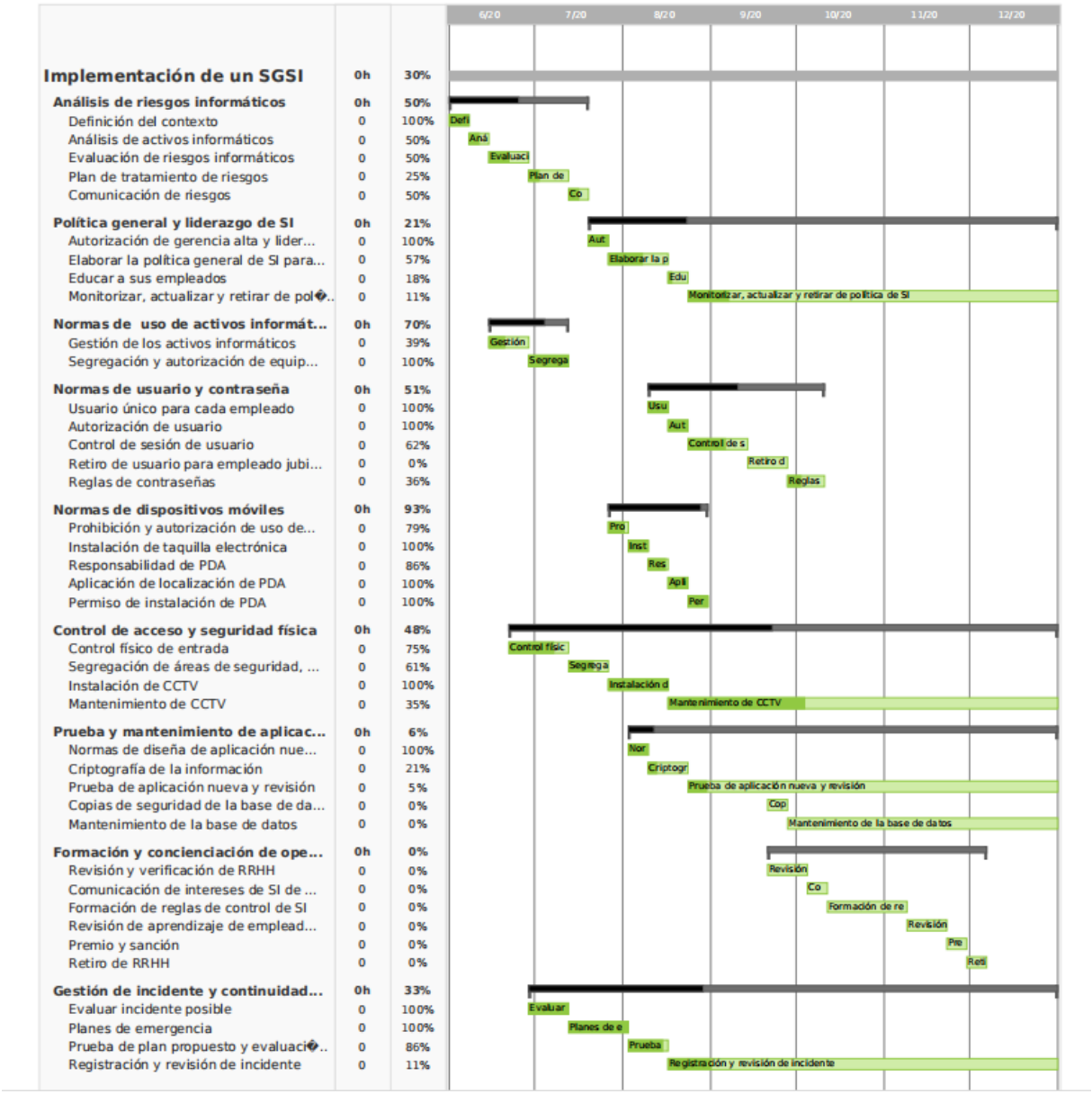
[4] En este proyecto se aplica TEAMGANTT para visualizar el plan de ejecución.

	2. Autorización de usuario	17-Aug-20	23-Aug-20	7	Director de RRHH de 4PX Iberia	100%
	3. Control de sesión de usuario	24-Aug-20	13-Sep-20	21	Dpto. IT de 4PX central	50%
	4. Retiro de usuario para empleado jubilado	14-Sep-20	27-Sep-20	14	Director de RRHH de 4PX Iberia	0%
	5. Reglas de contraseñas	28-Sep-20	11-Oct-20	14	Dpto. IT de 4PX central	25%
P-05	1. Prohibición y autorización de uso de móviles personas	27-Jul-20	2-Aug-20	7	Director de RRHH de 4PX Iberia	75%
	2. Instalación de taquilla electrónica	3-Aug-20	9-Aug-20	7	Grupo de IT de 4PX Iberia	100%
	3. Responsabilidad de PDA	10-Aug-20	16-Aug-20	7	Director de RRHH de 4PX Iberia	75%
	4. Aplicación de localización de PDA	17-Aug-20	23-Aug-20	7	Grupo de IT de 4PX Iberia	100%
	5. Permiso de instalación de PDA	24-Aug-20	30-Aug-20	7	Grupo de IT de 4PX Iberia	100%
P-06	1. Control físico de entrada	22-Jun-20	12-Jul-20	21	Grupo de IT de 4PX Iberia	75%
	2. Segregación de áreas de seguridad, acceso público, áreas de cargas y descargas	13-Jul-20	26-Jul-20	14	Gerente general de 4PX Iberia	50%
	3. Instalación de CCTV	27-Jul-20	16-Aug-20	21	Grupo de IT de 4PX Iberia	100%
	4. Mantenimiento de CCTV	17-Aug-20	31-Dec-20	137	Grupo de IT de 4PX Iberia	10%
P-07	1. Normas de diseña de aplicación nueva	3-Aug-20	9-Aug-20	7	Dpto. IT de 4PX central	25%
	2. Criptografía de la información	10-Aug-20	23-Aug-20	14	Dpto. IT de 4PX central	10%
	3. Prueba de aplicación nueva y revisión	24-Aug-20	31-Dec-20	130	Dpto. IT de 4PX central	10%
	4. Copias de seguridad de la base de datos, prueba de capacidad de carga	21-Sep-20	27-Sep-20	7	Dpto. IT de 4PX central	0%
	5. Mantenimiento de la base de datos	28-Sep-20	31-Dec-20	95	Dpto. IT de 4PX central	0%

P-08	1. Revisión y verificación de RRHH	21-Sep-20	4-Oct-20	14	Director de RRHH de 4PX Iberia	0%
	2. Comunicación de intereses de SI de 4PX Iberia	5-Oct-20	11-Oct-20	7	Director de RRHH de 4PX Iberia	0%
	3. Formación de reglas de control de SI	12-Oct-20	8-Nov-20	28	Grupo de IT de 4PX Iberia	0%
	4. Revisión de aprendizaje de empleados	9-Nov-20	22-Nov-20	14	Director de RRHH de 4PX Iberia	0%
	5. Premio y sanción	23-Nov-20	29-Nov-20	7	Director de RRHH de 4PX Iberia	0%
	6. Retiro de RRHH	30-Nov-20	6-Dec-20	7	Director de RRHH de 4PX Iberia	0%
P-09	1. Evaluar incidente posible	29-Jun-20	12-Jul-20	14	Grupo de IT de 4PX Iberia	75%
	2. Planes de emergencia	13-Jul-20	2-Aug-20	21	Grupo de IT de 4PX Iberia	75%
	3. Prueba de plan propuesto y evaluación	3-Aug-20	16-Aug-20	14	Grupo de IT de 4PX Iberia	75%
	4. Registración y revisión de incidente	17-Aug-20	31-Dec-20	137	Grupo de IT de 4PX Iberia	10%

Para ver la implantación del modelo de gestión de SI más directo, usamos el diagrama Gantt:

Fig.8. Proyectos de la implamtación del SGSI



Fuente: elaboración propia en la aplicación TeamGantt

Para cada proyecto propuesto, se ha hecho una carta de proyecto y un diagrama de fechas de ejecución.

5.2.1. Análisis de riesgos informáticos

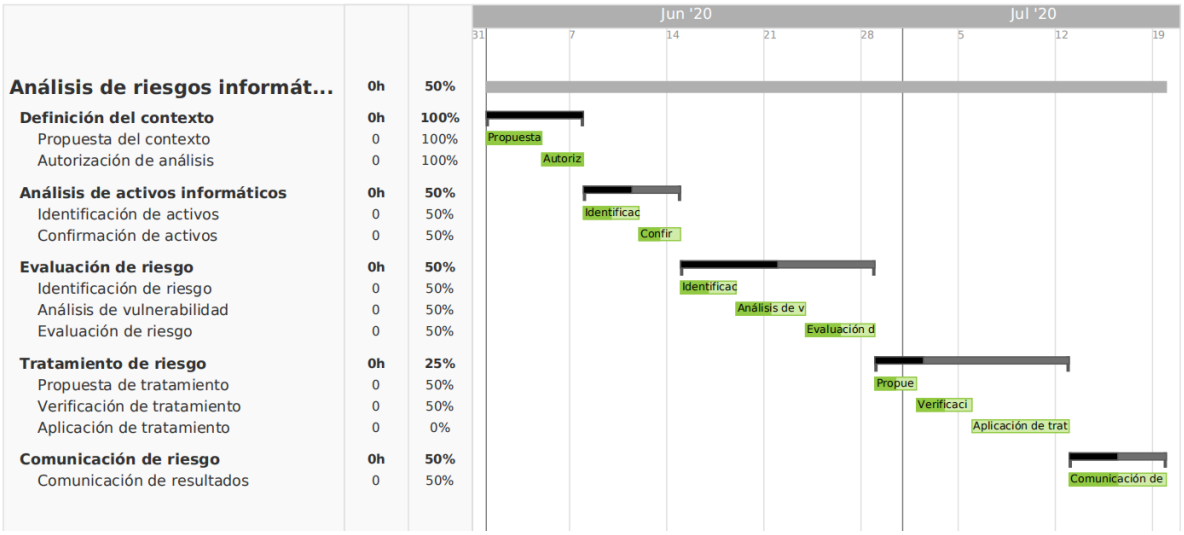
Tabla.16. Carta de proyecto de análisis de riesgos informáticos

N.º de Proyecto	P-01	Objetivo		Analizar y valorar riesgos de la información
Presupuesto	1000$	Tiempo de Implementación (días)		49
Tarea	Subtarea	Fecha inicial	Fecha final	Duración

Definición del contexto	Propuesta del contexto	1-Jun-20	4-Jun-20	4
	Autorización de análisis	5-Jun-20	7-Jun-20	3
Análisis de activos informáticos	Identificación de activos	8-Jun-20	11-Jun-20	4
	Confirmación de activos	12-Jun-20	14-Jun-20	3
Evaluación de riesgos	Identificación de riesgo	15-Jun-20	18-Jun-20	4
	Análisis de vulnerabilidad	19-Jun-20	23-Jun-20	5
	Evaluación de riesgo	24-Jun-20	28-Jun-20	5
Tratamiento de riesgos	Propuesta de tratamiento	29-Jun-20	1-Jul-20	3
	Verificación de tratamiento	2-Jul-20	5-Jul-20	4
	Aplicación de tratamiento	6-Jul-20	12-Jul-20	7
Comunicación de riesgos	Comunicación de resultados	13-Jul-20	19-Jul-20	7

4PX Iberia decide gastar 49 días para hacer el análisis de riesgos informáticos, a partir de 1 de junio hasta 19 de julio. Este proyecto tiene 5 subtareas: definición del contexto, análisis de activos informáticos, evaluación de riesgos, tratamiento de riesgos y comunicación de riesgos, va a gastar 1000$ para los recursos humanos.

Fig.9. Plan del análisis de riesgos informáticos



Fuente: elaboración propia en la aplicación TeamGantt

5.2.2. Política general y liderazgo de SI

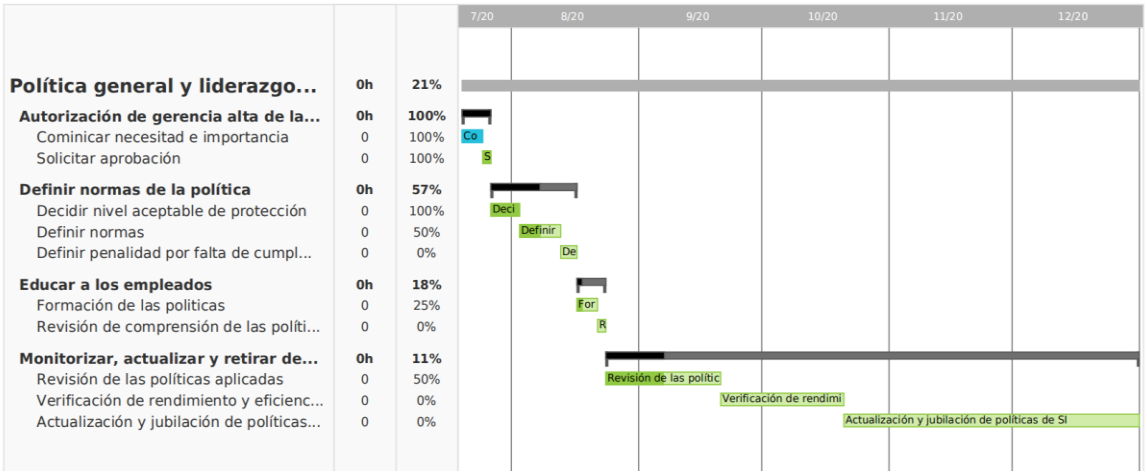
Tabla.17. Carta de proyecto de política general y liderazgo de SI

N.º de Proyecto	P-02	Objetivo		Establecer política general y liderazgo para SGSI
Presupuesto	4000$	Tiempo de Implementación (días)		165
Tarea	Subtarea	Fecha inicial	Fecha final	Duración

Autorización de gerencia alta de la empresa central	Comunicar necesitad e importancia	20-Jul-20	24-Jul-20	5
	Solicitar aprobación	25-Jul-20	26-Jul-20	2
Definir normas de la política	Decidir nivel aceptable de protección	27-Jul-20	02-Aug-20	7
	Definir normas	03-Aug-20	12-Aug-20	10
	Definir penalidad por falta de cumplimiento	13-Aug-20	16-Aug-20	4
Educar a los empleados	Formación de las políticas	17-Aug-20	21-Aug-20	5
	Revisión de comprensión de las políticas	22-Aug-20	23-Aug-20	2
Monitorizar, actualizar y retirar de política de SI Normas de seguridad teórica	Revisión de las políticas aplicadas	24-Aug-20	20-Sep-20	28
	Verificación de rendimiento y eficiencia	21-Sep-20	20-Oct-20	30
	Actualización y jubilación de políticas de SI	21-Oct-20	31-Dec-20	72

Este proyecto va a durar 165 días, desde que se termine el proyecto del análisis del riesgo hasta el fin del año 2020, va a gastar 4000$ para recursos humanos y algunas materias físicas.

Fig.10. Plan de la política general y liderazgo de SI



Fuente: elaboración propia en la aplicación TeamGantt

5.2.3. Normas de uso de activos informáticos

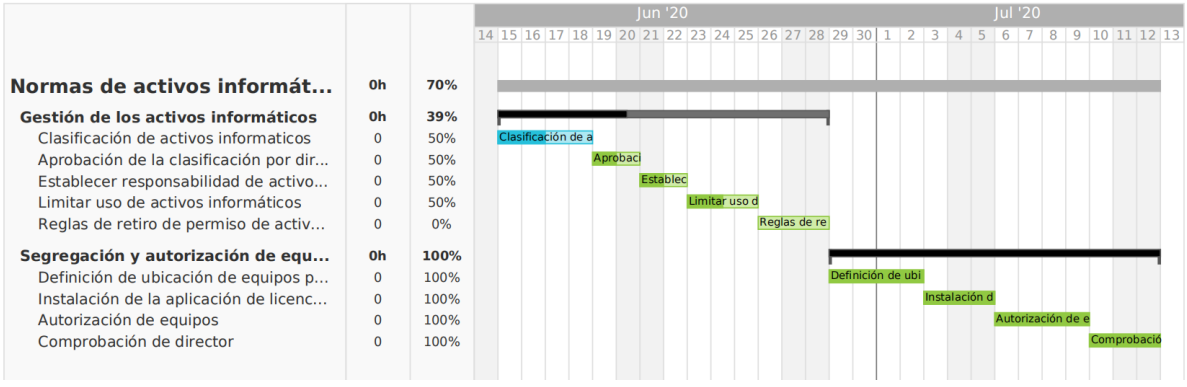
Tabla.18. Carta de proyecto normas de uso de activos informáticos

N.º de Proyecto	P-03	Objetivo	Identificar activos informáticos, establecer marcos teóricos del uso de equipos
Presupuesto	2000$	Tiempo de Implementación (días)	28

Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Gestión de los activos informáticos	Clasificación de activos informáticos	15-Jun-20	18-Jun-20	4
	Aprobación de la clasificación por director	19-Jun-20	20-Jun-20	2
	Establecer responsabilidad de activos informáticos	21-Jun-20	22-Jun-20	2
	Limitar uso de activos informáticos	23-Jun-20	25-Jun-20	3
	Reglas de retiro de permiso de activos para personas jubiladas	26-Jun-20	28-Jun-20	3
Segregación y autorización de equipos	Definición de ubicación de equipos para diferentes tareas	29-Jun-20	2-Jul-20	4
	Instalación de la aplicación de licencia	3-Jul-20	5-Jul-20	3
	Autorización de equipos	6-Jul-20	9-Jul-20	4
	Comprobación de director	10-Jul-20	12-Jul-20	3

Este proyecto va a durar 28 días, de 15 de junio a 12 de julio, va a gastar 2000$ para los recursos humanos en 4PX Iberia[5].

Fig.11. Plan de las normas de uso de activos informáticos



Fuente: elaboración propia en la aplicación TeamGantt

5.2.4. Normas de usuario y contraseña

Tabla.19. Carta de proyecto normas de usuario y contraseña

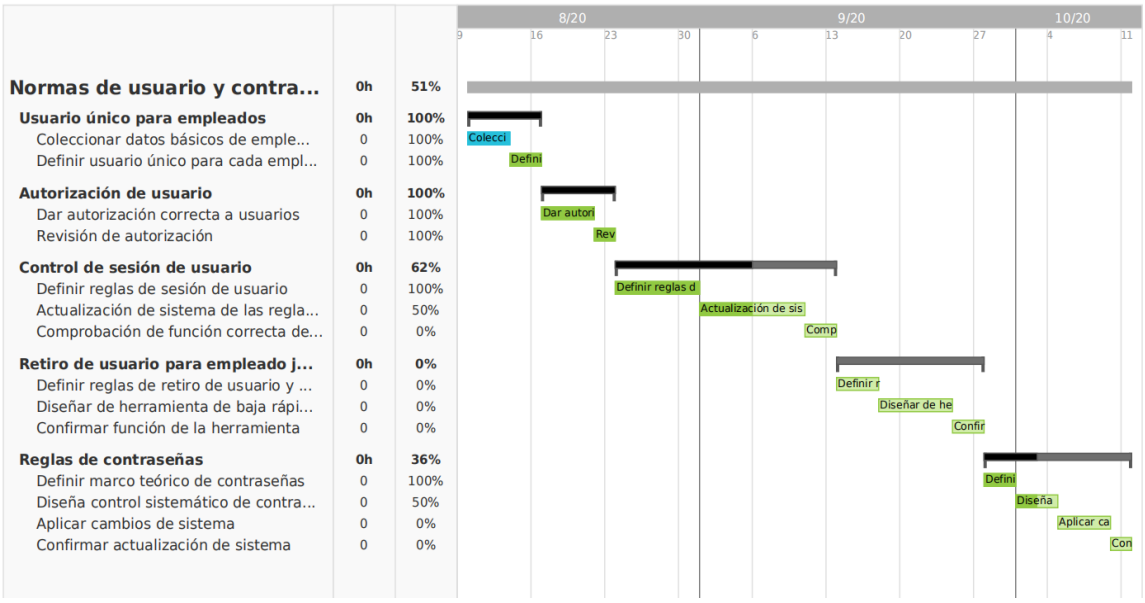
N.º de Proyecto	P-04	Objetivo	Establecer uso correcto de usuarios y contraseñas

[5] El coste para un empleado de tiempo completo en 4PX Iberia es unos 1800$ al mes.

Presupuesto	4000$	Tiempo de Implementación (días)		60
Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Usuario único para empleados	Coleccionar datos básicos de empleados	13-Jul-20	16-Jul-20	4
	Definir usuario único para cada empleado	17-Jul-20	19-Jul-20	3
Autorización de usuario	Dar autorización correcta a usuarios	20-Jul-20	24-Jul-20	5
	Revisión de autorización	25-Jul-20	26-Jul-20	2
Control de sesión de usuario	Definir reglas de sesión de usuario	24-Aug-20	30-Aug-20	7
	Actualización de sistema de las reglas de usuario	31-Aug-20	9-Sep-20	10
	Comprobación de función correcta del sistema	10-Sep-20	13-Sep-20	4
Retiro de usuario para empleado jubilado	Definir reglas de retiro de usuario y su autorización	14-Sep-20	17-Sep-20	4
	Diseñar de herramienta de baja rápida de usuario	18-Sep-20	24-Sep-20	7
	Confirmar función de la herramienta	25-Sep-20	27-Sep-20	3
Reglas de contraseñas	Definir marco teórico de contraseñas	13-Aug-20	15-Aug-20	3
	Diseña control sistemático de contraseñas	16-Aug-20	19-Aug-20	4
	Aplicar cambios de sistema	20-Aug-20	24-Aug-20	5
	Confirmar actualización de sistema	25-Aug-20	26-Aug-20	2

Este proyecto va a durar 60 días, de 13 de julio a 26 de agosto, va a gastar 4000$ para los recursos humanos en 4PX Iberia y unos miembros del departamento informático en la empresa matriz.

Fig.12. Plan de las normas de usuario y contraseña



Fuente: elaboración propia en la aplicación TeamGantt

5.2.5. Normas de dispositivos móviles

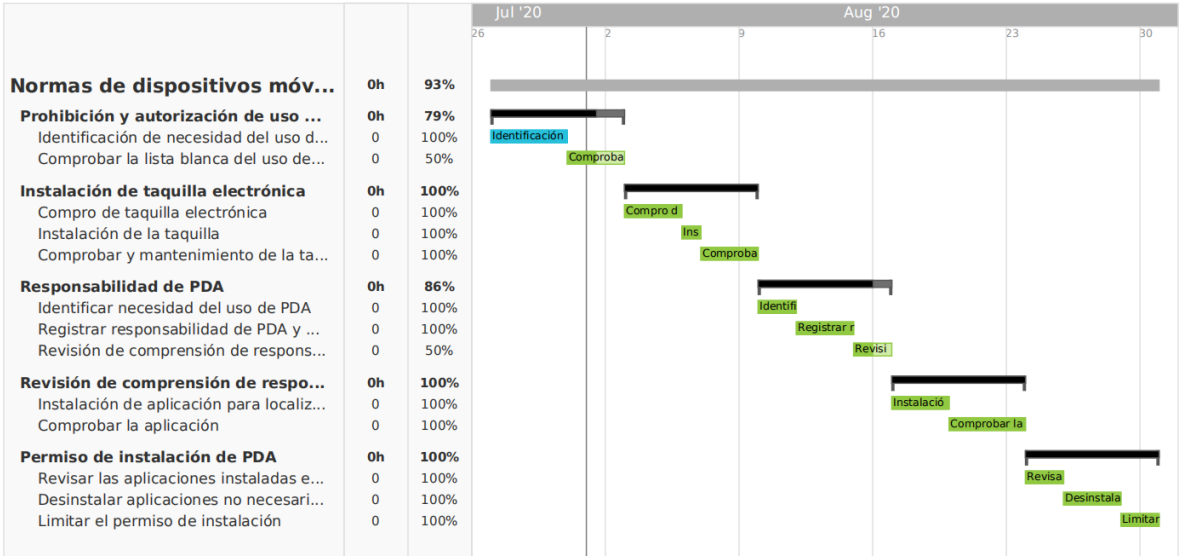
Tabla.20. Carta de proyecto de las Normas de dispositivos móviles

N.º de Proyecto	P-05	Objetivo		Controlar el uso de móviles personales y PDA
Presupuesto	3000$	Tiempo de Implementación (días)		35
Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Prohibición y autorización de uso de móviles personas	Identificación de necesidad del uso de móvil personal	13-Jul-20	16-Jul-20	4
	Comprobar la lista blanca del uso de móvil personal	17-Jul-20	19-Jul-20	3
Instalación de taquilla electrónica	Compro de taquilla electrónica	20-Jul-20	22-Jul-20	3
	Instalación de la taquilla	23-Jul-20	23-Jul-20	1
	Comprobar y mantenimiento de la taquilla	24-Jul-20	26-Jul-20	3
Responsabilidad de PDA	Identificar necesidad del uso de PDA	10-Aug-20	11-Aug-20	2
	Registrar responsabilidad de PDA y publicar normas de uso	12-Aug-20	14-Aug-20	3
	Revisión de comprensión de responsabilidad de PDA	15-Aug-20	16-Aug-20	2

Revisión de comprensión de responsabilidad de PDA	Instalación de aplicación para localizar PDA	17-Aug-20	19-Aug-20	3
	Comprobar la aplicación	20-Aug-20	23-Aug-20	4
Permiso de instalación de PDA	Revisar las aplicaciones instaladas en PDA	17-Aug-20	20-Aug-20	4
	Desinstalar aplicaciones no necesarias	17-Aug-20	20-Aug-20	4
	Limitar el permiso de instalación	21-Aug-20	23-Aug-20	3

Este proyecto dura 35 días, de 13 de julio a 23 de agosto, va a gastar 2000$ para los recursos humanos, 500$ para las taquillas electrónicas y 500$ para las aplicaciones en PDA.

Fig.13. Plan de las Normas de dispositivos móviles



Fuente: elaboración propia en la aplicación TeamGantt

5.2.6. Control de acceso y seguridad física

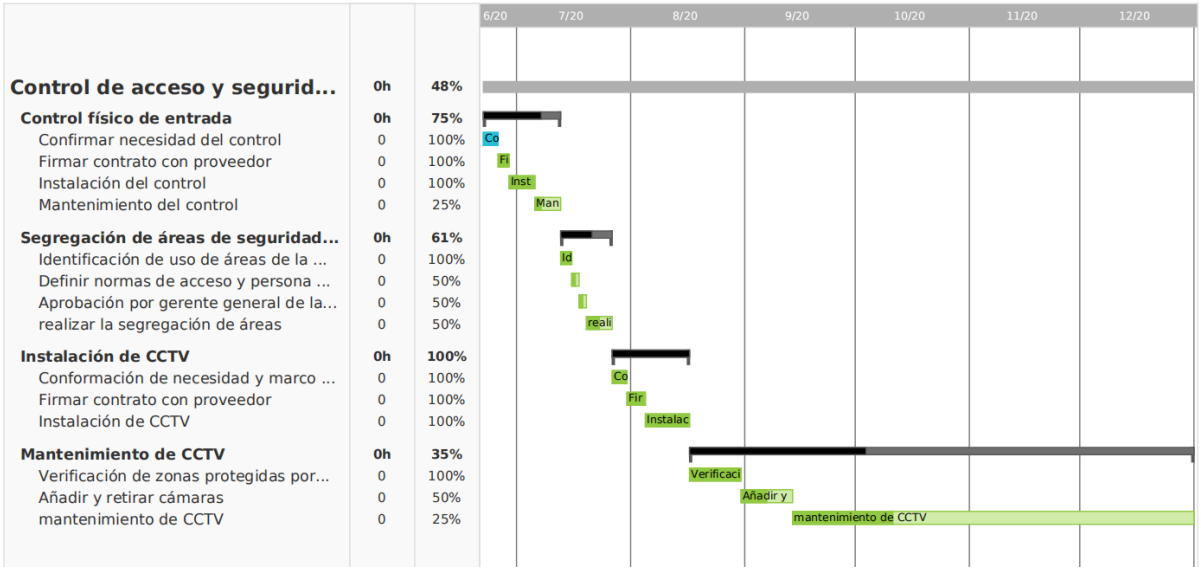
Tabla.21. Carta de proyecto de control de acceso y seguridad física

N.º de Proyecto	P-06	Objetivo		Establecer normas de acceso y gestionar seguridad física
Presupuesto	2,5000$	Tiempo de Implementación (días)		232
Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Control físico de entrada	Confirmar necesidad del control	22-Jun-20	25-Jun-20	4
	Firmar contrato con proveedor	26-Jun-20	28-Jun-20	3
	Instalación del control	29-Jun-20	5-Jul-20	7

	Mantenimiento del control	6-Jul-20	12-Jul-20	7
Segregación de áreas de seguridad, acceso público, áreas de cargas y descargas	Identificación de uso de áreas de la empresa	13-Jul-20	15-Jul-20	3
	Definir normas de acceso y persona de responsabilidad	16-Jul-20	17-Jul-20	2
	Aprobación por gerente general de la empresa	18-Jul-20	19-Jul-20	2
	realizar la segregación de áreas	20-Jul-20	26-Jul-20	7
Instalación de CCTV	Conformación de necesidad y marco legal de la instalación	6-Jul-20	9-Jul-20	4
	Formar contrato con proveedor	10-Jul-20	14-Jul-20	5
	Instalación de CCTV	15-Jul-20	26-Jul-20	12
Mantenimiento de CCTV	Verificación de zonas protegidas por CCTV	27-Jul-20	9-Aug-20	14
	Añadir y retirar cámaras	10-Aug-20	23-Aug-20	14
	mantenimiento de CCTV	24-Aug-20	31-Dec-20	130

Este proyecto va a durar 232, desde el 22 de junio hasta el fin del año, va a gastar 10000$ para el control de entrada, 10000$ para la instalación de CCTV y 5000$ para los recursos humanos y el mantenimiento de equipos.

Fig.14. Plan del control de acceso y seguridad física



Fuente: elaboración propia en la aplicación TeamGantt

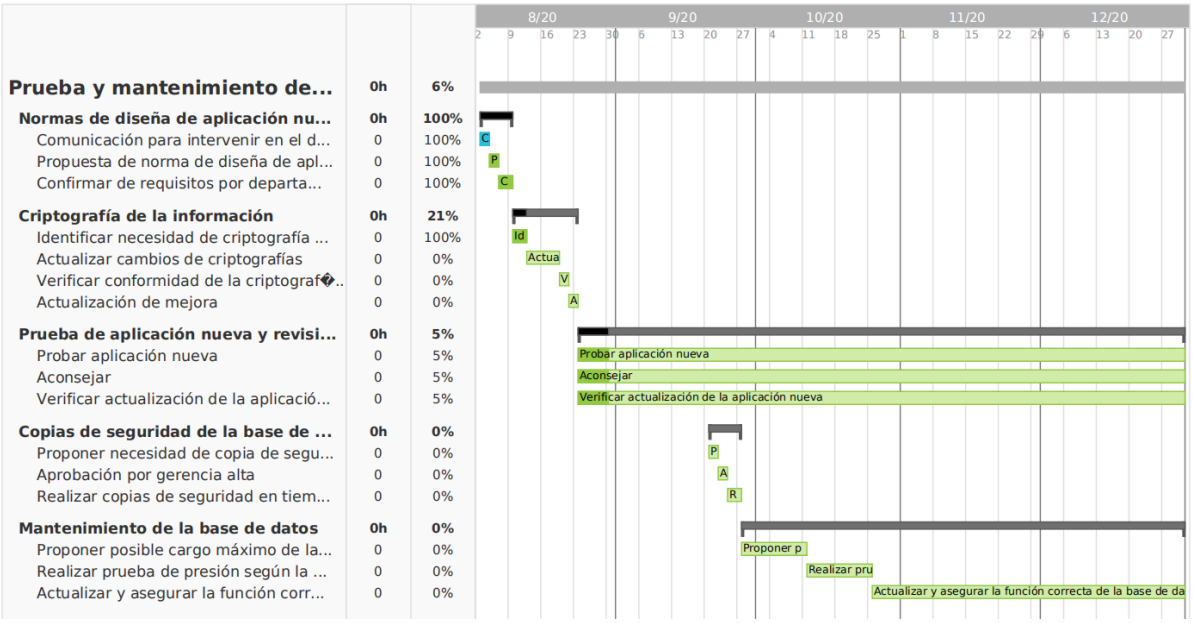
5.2.7. Prueba y mantenimiento de aplicaciones y servidor

Tabla.22. Carta de proyecto de prueba y mantenimiento de aplicaciones y servidor

N.º de Proyecto	P-07	Objetivo		Asegurar seguridad de la aplicación y base de datos
Presupuesto	4000$	Tiempo de Implementación (días)		151
Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Normas de diseña de aplicación nueva	Comunicación para intervenir en el diseño de aplicación	3-Aug-20	4-Aug-20	2
	Propuesta de norma de diseña de aplicación	5-Aug-20	6-Aug-20	2
	Confirmar de requisitos por departamento IT de la empresa central	7-Aug-20	9-Aug-20	3
Criptografía de la información	Identificar necesidad de criptografía de la información	10-Aug-20	12-Aug-20	3
	Actualizar cambios de criptografías	13-Aug-20	19-Aug-20	7
	Verificar conformidad de la criptografía de la información en los procesos de producción	20-Aug-20	21-Aug-20	2
	Actualización de mejora	22-Aug-20	23-Aug-20	2
Prueba de aplicación nueva y revisión	Probar aplicación nueva	24-Aug-20	31-Dec-20	130
	Aconsejar	24-Aug-20	31-Dec-20	130
	Verificar actualización de la aplicación nueva	24-Aug-20	31-Dec-20	130
Copias de seguridad de la base de datos, prueba de capacidad de carga	Proponer necesidad de copia de seguridad	21-Sep-20	22-Sep-20	2
	Aprobación por gerencia alta	23-Sep-20	24-Sep-20	2
	Realizar copias de seguridad en tiempo real	25-Sep-20	27-Sep-20	3
Mantenimiento de la base de datos	Proponer posible cargo máximo de la base de datos	28-Sep-20	11-Oct-20	14
	Realizar prueba de presión según la predicción	12-Oct-20	25-Oct-20	14
	Actualizar y asegurar la función correcta de la base de datos	26-Oct-20	31-Dec-20	67

Este proyecto va a durar 151 días, de 3 de agosto al fin del año, va a gastar 4000$ para los recursos humanos.

Fig.15. Plan de la prueba y mantenimiento de aplicaciones y servidor



Fuente: elaboración propia en la aplicación TeamGantt

5.2.8. Formación y concienciación de operadores

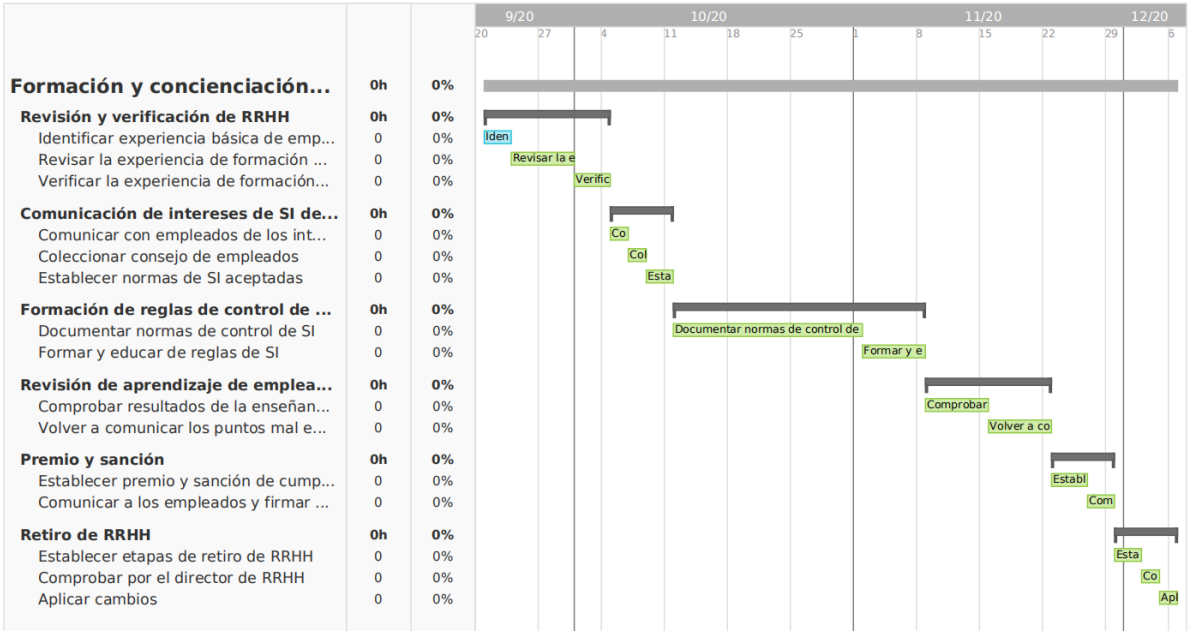
Tabla.23. Carta de proyecto la formación y concienciación de operadores

N.º de Proyecto	P-08	Objetivo		Garantizar seguridad de RRHH de la organización
Presupuesto	2000$	Tiempo de Implementación (días)		63
Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Revisión y verificación de RRHH	Identificar experiencia básica de empleados	21-Sep-20	23-Sep-20	3
	Revisar la experiencia de formación de empleados	24-Sep-20	30-Sep-20	7
	Verificar la experiencia de formación de personas entrevistada	1-Oct-20	4-Oct-20	4
Comunicación de intereses de SI de 4PX Iberia	Comunicar con empleados de los intereses de SI	5-Oct-20	6-Oct-20	2
	Coleccionar consejo de empleados	7-Oct-20	8-Oct-20	2
	Establecer normas de SI aceptadas	9-Oct-20	11-Oct-20	3
Formación de reglas de control de SI	Documentar normas de control de SI	12-Oct-20	1-Nov-20	21

	Formar y educar de reglas de SI	2-Nov-20	8-Nov-20	7
Revisión de aprendizaje de empleados	Comprobar resultados de la enseñanza de reglas de SI	9-Nov-20	15-Nov-20	7
	Volver a comunicar los puntos mal entendidos	16-Nov-20	22-Nov-20	7
Premio y sanción	Establecer premio y sanción de cumplimiento de reglas de SI	9-Nov-20	12-Nov-20	4
	Comunicar a los empleados y firmar documentos de compromiso	13-Nov-20	15-Nov-20	3
Retiro de RRHH	Establecer etapas de retiro de RRHH	16-Nov-20	18-Nov-20	3
	Comprobar por el director de RRHH	19-Nov-20	20-Nov-20	2
	Aplicar cambios	21-Nov-20	22-Nov-20	2

Este proyecto dura 63 días, de 21 de septiembre a 22 de noviembre. Solo va a gastar 2000$ porque no va a ocupar mucho tiempo del grupo informático de 4PX Iberia.

Fig.16. Plan de la formación y concienciación de operadores



Fuente: elaboración propia en la aplicación TeamGantt

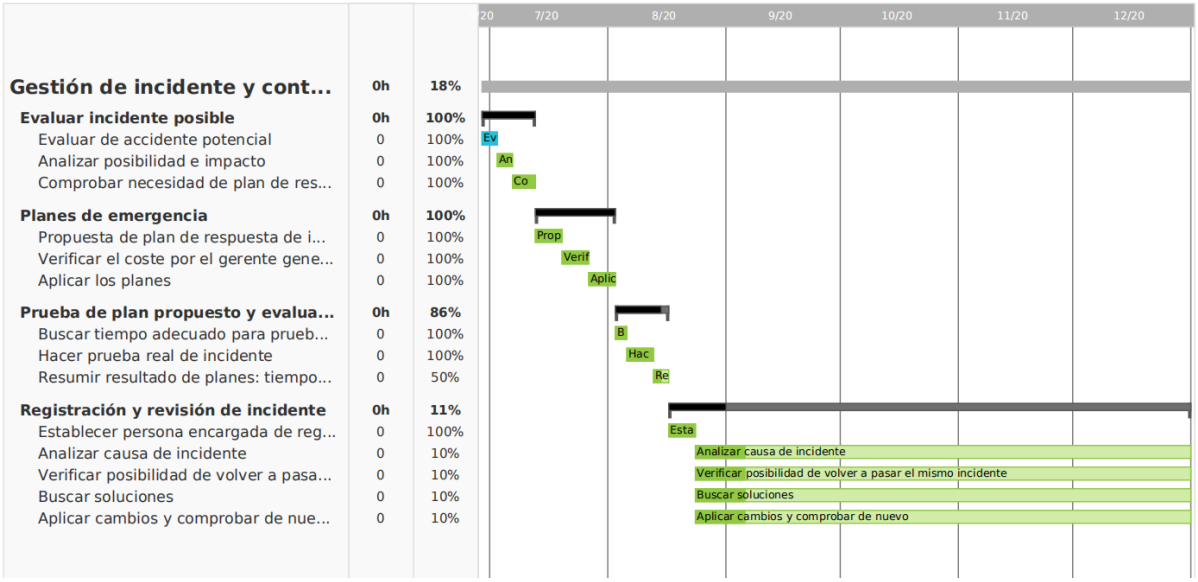
5.2.9. Gestión de incidente y continuidad de negocio

Tabla.24. Carta de proyecto de la gestión de incidente y continuidad de negocio

N.º de Proyecto	P-09	Objetivo		Establecer planes de continuidad de negocio y mejora continua de SGSI
Presupuesto	3000$	Tiempo de Implementación (días)		172
Tarea	Subtarea	Fecha inicial	Fecha final	Duración
Evaluar incidente posible	Evaluar de accidente potencial	29-Jun-20	2-Jul-20	4
	Analizar posibilidad e impacto	3-Jul-20	6-Jul-20	4
	Comprobar necesidad de plan de respuesta	7-Jul-20	12-Jul-20	6
Planes de emergencia	Propuesta de plan de respuesta de incidencia	13-Jul-20	19-Jul-20	7
	Verificar el coste por el gerente general de 4PX Iberia	20-Jul-20	26-Jul-20	7
	Aplicar los planes	27-Jul-20	2-Aug-20	7
Prueba de plan propuesto y evaluación	Buscar tiempo adecuado para pruebas de plan propuesto	3-Aug-20	5-Aug-20	3
	Hacer prueba real de incidente	6-Aug-20	12-Aug-20	7
	Resumir resultado de planes: tiempo de recupera, eficiencia infectada	13-Aug-20	16-Aug-20	4
Registración y revisión de incidente	Establecer persona encargada de registrar incidente	31-Aug-20	6-Sep-20	7
	Analizar causa de incidente	7-Sep-20	31-Dec-20	116
	Verificar posibilidad de volver a pasar el mismo incidente	7-Sep-20	31-Dec-20	116
	Buscar soluciones	7-Sep-20	31-Dec-20	116
	Aplicar cambios y comprobar de nuevo	7-Sep-20	31-Dec-20	116

Este proyecto va a durar 172 días, de 29 de junio al fin del año, va a gastar 3000$ para los recursos humanos y algunas materias para los planes de emergencia; por ejemplo las baterías para el caso de corte de luz.

Fig.17. Plan de la gestión de incidente y continuidad de negocio



Fuente: elaboración propia en la aplicación TeamGantt

En conclusión, el proyecto de la implantación del SGSI en 4PX Iberia va a durar 7 meses, de 1 de junio a 31 de diciembre del año 2020; el presupuesto total es **48,000$**.

5.3. Auditoria de calidad del proyecto

Para evaluar los resultados de los proyectos, se aplica el modelo CMMI, clasificando los rendimientos en 5 niveles:

- **Inicial**

Se ha terminado el proyecto, han conseguido el objetivo básico.

- **Gestionado**

La organización tiene recursos preparados para el proyecto, tiene un buen control de los procesos del proyecto.

- **Definido**

Se han clasificado bien las reglas de la implementación del proyecto, se han clasificado los procesos para aplicar el proyecto en otro entorno.

- **Cuantitativamente gestionado**

Se han identificado los controles cuantitativos para evaluar el proyecto, el administrador puede tener una valoración fácil y objetiva.

- **Optimizado**

Han evaluado bien los procesos y resultados del proyecto, tienen actualizaciones adecuadas y mejoras continuas.

El objetivo básico de estos proyectos es llegar al nivel gestionado; para los activos informáticos y la seguridad informática, la empresa tiene que establecer una persona de responsabilidad; los procesos de los proyectos tienen que estar bien definidos y realizados. Al final de cada proyecto, se va a hacer una encuesta a todos los empleados, para comprobar los rendimientos del proyecto.

6. Resultados

6.1. Análisis de riesgos

Se puede observar que como 4PX Iberia es una empresa de almacenaje y distribución de paquetes, no solo sus productos tienen alto nivel de seguridad física, sino que sus activos informáticos tienen un buen nivel de **seguridad física** también. Pero hay que tener en cuenta que casi no tiene ningún control dirigido a la gestión de la seguridad informática, ni siquiera hay una persona encargada de administrar la SI en esta empresa.

Según el análisis de riesgos informáticos de la empresa, las vulnerabilidades de la empresa son:

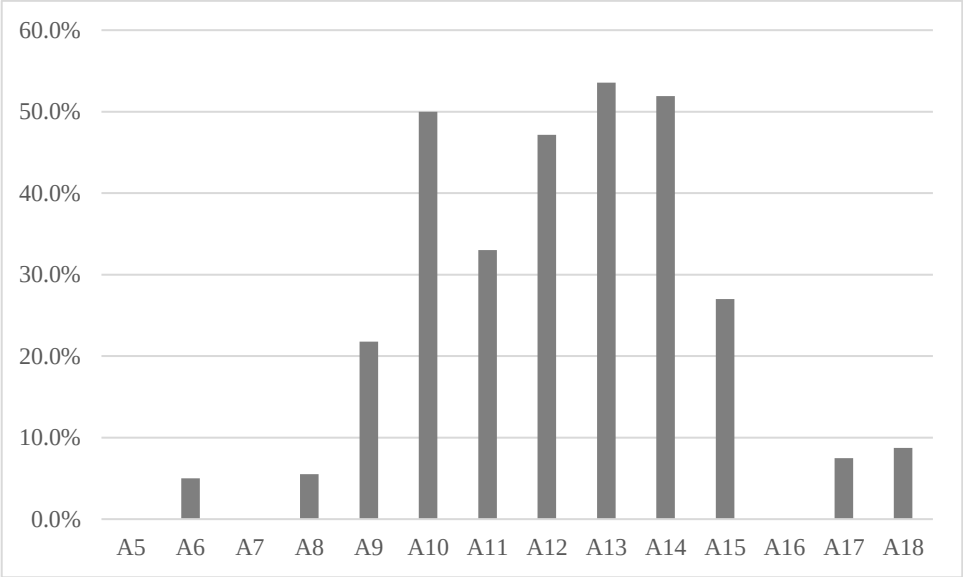
Tabla.25. Resumen de vulnerabilidades de 4PX Iberia

N.º de vulnerabilidad	Descripción	Valoración
Vul-01	Factor natural o social	Ligera
Vul-02	Error o descuido de trabajadores	Grave
Vul-03	fallos de software y/o hardware	Ligera
Vul-04	abuso de autorización o acceso prohibido	Ligera
Vul-05	ataque interno y/o externo	Mediana
Vul-06	gestión inadecuada de la organización	Muy Grave
Vul-07	intrusión física y/o robo	Ligera
Vul-08	fallos de suministro	Ligera

En primer lugar, una vulnerabilidad muy grave de la empresa es la gestión inadecuada de la organización; para reducir el riesgo de la compañía, hay que establecer liderazgo y política general de la SI. Luego dicha empresa tiene que buscar normas adecuadas de gestión de los activos informáticos y acciones de producción. En segundo lugar, la vulnerabilidad grave de la empresa es la alta probabilidad de error o descuido de trabajadores; para evitar este problema, se puede consolidar la importancia de la formación y el conocimiento de las reglas de gestión de la SI. En tercer lugar, la vulnerabilidad mediana de la empresa es la falta de medidas para prevenir un ataque interno y/o externo, Para minimizar el riesgo, por un lado, hay que segregar zonas de trabajo y equipos de diferentes tareas; por otro lado, hay que revisar y actualizar las aplicaciones de producción. En el último lugar, los riesgos ligeros se pueden reducir, transferir o asumir según su impacto y probabilidad.

Tras el análisis de riesgo, se ha hecho una encuesta de los controles de las normas de ISO/IEC 27001 para tener una visión profesional de los riesgos de la empresa. Clasificamos los niveles de cumplimientos de los controles en 6 niveles: Inexistente (0%), Inicial (10%), Definido (25%), Procesando (50%), Administrado (75) y Optimizado (100%), los resultados son:

Fig.18. Cumplimiento de dominios de ISO 27001



Fuente: elaboración propia

Según esta encuesta del estado del nivel de la SI de la empresa, se ve muy claro que 4PX Iberia tiene deficiencias en la estructura de la seguridad informática.

En conclusión, el proyecto de establecer liderazgo y políticas de la SI en 4PX Iberia es **muy urgente**.

6.2. Proyecto de implantación del SGSI

Los proyectos propuestos para esta empresa tienen estos objetivos:

1. Establecer la organización de gestión de SI en esta empresa.
2. Reconocer sus activos informáticos
3. Buscar marcos teóricos de protección de estos activos
4. Consolidar sus rendimientos de seguridad física
5. Formar y comunicar la SI a sus empleados
6. Plan continuo de negocio en caso de contingencia

La implementación de los proyectos va a suponer 7 meses y 48,000$.

6.3. Calidad de proyectos

Después de realizar el proyecto de implantación del SGSI en la empresa, empezamos a evaluar los rendimientos. Aplicamos el modelo CMMI y clasificamos los resultados en 5 niveles: Inicial, Gestionado, Definido, Cuantitativamente Gestionado y Optimizado.

El objetivo básico del proyecto es conseguir el nivel gestionado; es decir, después del proyecto, la empresa tiene que tener los activos informáticos controlados, los empleados tienen que saber su responsabilidad en la seguridad informática y solo hacer operaciones permitidas en las normas.

El objetivo avanzado es tener el nivel definido; cuando 4PX Iberia tenga su SGSI funcionando bien, seguirán mejorando continuamente su SGSI y podrán aplicar el modelo de 4PX Iberia en otras subsidiarias de la empresa matriz.

El objetivo más avanzado es tener el nivel cuantitativamente gestionado; el director de la SI puede valorar los resultados de la SGSI según las normas cuantitativas para conseguir un resultado objetivo y correcto.

- **Rendimientos del proyecto**

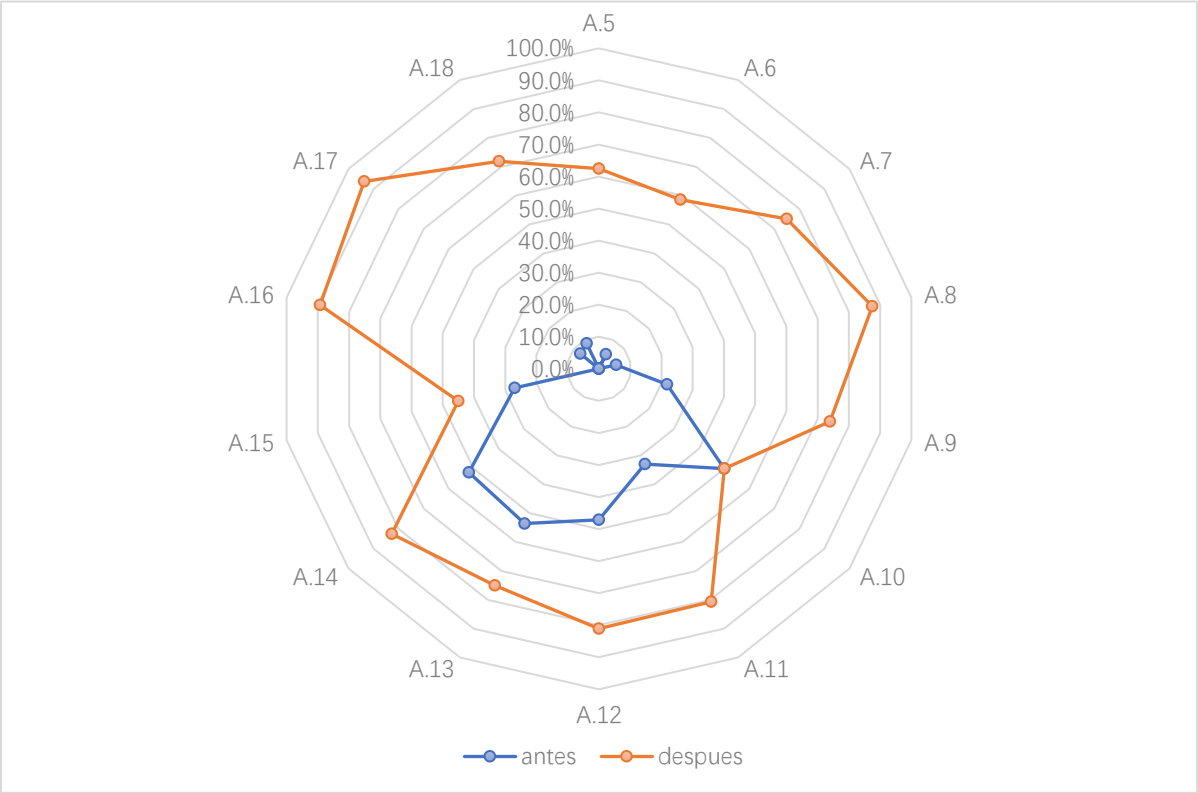
Después del proyecto, hacemos una encuesta de los controles de ISO 27001 otra vez a verificar los resultados del proyecto.[6]

Tabla.26. Resultado esperado del proyecto en los controles de ISO 27001

Cumplimiento	Inexistente	Inicial	Definido	Procesando	Administrado	Optimizado
Resumen de los puntos	2	4	4	13	46	45

Para ver los resultados de una forma directa, usamos el diagrama radio:

Fig.19. Cambios de resultados de controles de ISO/IEC 27001



Fuente: elaboración propia

6.4. Modelo de gestión de seguridad informática para 4PX Iberia

En resumen, este modelo de gestión de seguridad informática tiene 3 niveles:

- **Nivel 1: liderazgo y responsabilidad de la SI**

Decide las personas de liderazgo de la SI, clasifica su responsabilidad.

- **Nivel 2: Política general de la SI**

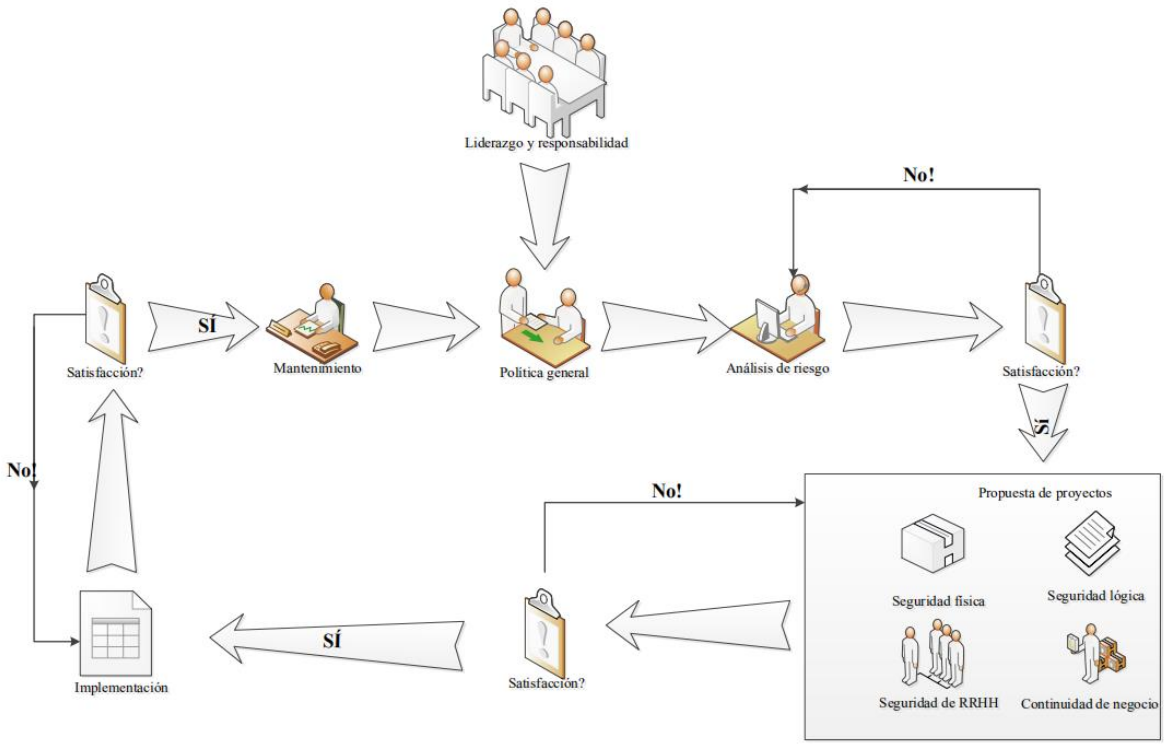
Identifica la política general de la SI, propone necesidad actual de la SI en la empresa.

- **Nivel 3: Normas de seguridad lógica, normas de seguridad física, formación de la SI y continuidad de negocio**

Planificar e implementar proyectos de gestión de la SI en estos 4 dominios. Verificar sus resultados.

[6] Los detalles están en el Anexo A

Fig.20. Modelo de gestión de seguridad informática



Fuente: elaboración propia

Se puede observar en la figura que el modelo de la gestión de la SI en la empresa también cumple los ciclos de mejora continua; la propuesta, análisis y propuesta de proyectos son la etapa Plan, la implementación es la etapa Do, el mantenimiento es la etapa Check, la propuesta de la nueva política general de la empresa es Act. Por tanto, la implementación del modelo SGSI en la empresa no es un trabajo único, sino que es un trabajo continuo para conseguir una constante seguridad informática en la empresa.

7. Líneas futuras

Este apartado define posibles trabajos futuros de ampliación del proyecto. Consta de dos partes: certificación de ISO 27001 y aplicación del modelo en más empresas similares.

7.1. Certificación de ISO 27001

Tras implantar el SGSI en la empresa, a partir del año 2021, ya se puede empezar a solicitar la certificación ISO/IEC 27001. La empresa tardará 6 meses para conseguir la certificación ISO 27001; la solicitud tiene estas tapas:

1. Análisis y evaluación de riesgos
2. Establecimiento de liderazgo y definición de política de seguridad informática
3. Plan de tratamiento de riesgos y mejora continua
4. Implementación de controles de seguridad informática
5. Preparación de documentos de certificación
6. Primera solicitud de certificación
7. Evaluación y consejos de mejora
8. Actualización de controles de seguridad informática
9. Segunda solicitud
10. Evaluación y actualización final
11. Certificación y mantenimientos

El coste para la certificación ISO 27001 será unos 15, 000 $; tiene dos partes: 4,000 $ son para las solicitudes de certificación y 11,000 $ son para los recursos humanos y físicos de la preparación.

La certificación ISO 27001 le sirve a 4PX Iberia en muchos puntos:

En primer lugar, la certificación reconoce los esfuerzos y rendimientos del control de seguridad informática de la empresa; justifica la capacidad de gestionar sus activos informáticos y protección de los datos secretos.

En segundo lugar, asegura la continuidad de desarrollo de la empresa; sin preocupación de fallos del apoyo del sistema informático, el crecimiento del negocio será más rápido.

En tercer lugar, consolida los conocimientos de la importancia de la seguridad informática, coordina todos los empleados de dicha empresa.

En cuarto lugar, gana confianza externa y mejora la competitividad de la empresa.

En el último lugar, evita riesgos legales.

7.2. Modelo de gestión de SI para empresas similares

Ahora muchas compañías chinas están abriendo almacenes extranjeros, muchos vendedores en línea tiene naves en Alemania, Francia e Inglaterra para garantizar transporte rápido y el servicio posventa; ahora en España hay tres empresas similares a la empresa 4PX Iberia; la empresa matriz 4PX tiene otras 12 subsidiarias por todo el mundo. Por tanto, el mercado de este modelo de gestión de seguridad informática es muy grande.

Si el modelo funciona bien en España, por un lado, el grupo de gestión de seguridad informática puede seguir desarrollando el modelo mientras el crecimiento de la empresa; por otro lado, pueden aplicar el modelo de 4PX Iberia en otras subsidiarias de 4PX incluso vender el modelo a otras empresas similares. La empresa S.F. Exprés, el líder del envío exprés en China, el año 2019 ha celebrado su tercera reunión de seguridad informática en Shenzhen el sur de China[7]; ya no solo vende sus servicios de paquetes urgentes, también vende su modelo de

[7] Noticia de la reunión de S.F. Exprés http://talk.cri.cn/n/20190711/4031cd60-d319-33d1-530b-6cd1fb77a849.html

control de seguridad informática. 4PX Iberia puede aprender la forma de negocio de dicha empresa y aplicarlo en España.

8. Conclusiones

1. 4PX Iberia tiene un buen control de la seguridad física pero casi no tiene más medidas para asegurar la seguridad informática. Según las normas de ISO/IEC 27001:2013, seguridad física solo es un dominio entre los 14 dominios de revisión. Considerando el crecimiento explosivo del negocio de 4PX Iberia, la necesidad de un control completo de la seguridad informática es más urgente cada día.
2. Un análisis de riesgos informáticos es la base del SGSI para una organización. No hay recursos ilimitados para la implementación del SGSI, por tanto, saber qué vulnerabilidad es más urgente y qué amenaza tiene valor más alto nos ayuda a organizar el trabajo de la implementación y decidir el nivel de esfuerzo invertido para lograr los objetivos.
3. Los 14 dominios de las normas ISO/IEC 27001 nos ofrecen una buena clasificación de los campos de gestión de la SI; incluyen estos aspectos importantes del SGSI para una organización:
   - Política de seguridad, liderazgo y responsabilidad de SGSI
   - Identificación de los activos de la información, normas de uso de estos activos.
   - Control de acceso físico y sistemático
   - Criptografía
   - Seguridad de dispositivos, seguridad de comunicación, seguridad de aplicación y la base de datos
   - Relación con proveedor
   - Seguridad de RRHH
   - Plan continuo de negocio
   - Marco legal de gestión de la SI
4. Un SGSI basando en ISO/IEC 27001:2013 puede tener mejor clasificación de tareas y objetivos más claro. Durante los procesos de la implementación del SGSI, los indicadores a considerar son muy importantes. Los indicadores tienen que ser fáciles de obtener y mensurables, para que el grupo de administración de la implementación puede ver los cambios de proyectos y valorar el éxito o fracaso.
5. Archivar los documentos de SGSI es muy importante, cumplir la implementación del SGSI no es el fin del trabajo. A través de analizar los cambios de los proyectos, los errores de los proyectos y las mejoras de la propuesta, podemos obtener un modelo más eficaz y adecuado para la organización. Esto también cumple el ciclo de mejora continua PDCA de las normas de 27000.
6. El apoyo de la gerencia alta es el factor más importante de la implementación de un SGSI; cuando todo el mundo puede coordinarse para lograr el objetivo, el trabajo va a ser más productivo y ejecutivo.

9. Bibliografía

1. *How Chinese Cybersecurity Standards Impact Doing Business in China, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china (17-08-2020)*
2. *Gestión del riesgo de las TI NTC 27005 https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI9.pdf (17-08-2020)*
3. *Metodología para la gestión de la seguridad informática https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf (12-08-2020)*
4. *ISO/IEC 27001: PDCA http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html (11-08-2020)*
5. *MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN GEOCONSULT CS https://repository.ean.edu.co/bitstream/handle/10882/9521/FonsecaOmar2019.pdf;jsessionid=DFF446FC26F93FB0B30ACB1C8A1DF9DB?sequence=1 (13-08-2020)*
6. *PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013 http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf (13-08-2020)*
7. *¿Por qué necesitamos un SGSI? https://www.semic.es/es/content/por-que-necesitamos-un-sgsi (11-08-2020)*
8. *WHITEPAPER ISO/IEC 27005 https://pecb.com/pdf/whitepapers/31-white-papers-iso-27005.pdf (17-08-2020)*
9. *Implementación SGSI EMPRESA POLLOS PACHITO S.A. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43110/1/rruizmutfm0615.pdf (20-08-2020)*
10. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*
11. *Ejemplo de Análisis de Riesgos (01-08-2020) http://omarbenjumea.blogspot.com/2014/07/ejemplo-de-analisis-de-riesgos.html (05-08-2020)*
12. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf (07-08-2020)*

Anexos

Anexo A, análisis completo según los controles de ISO/IEC 27001

Resultados de los controles de ISO 27001 antes del proyecto

N.º	Cumplimiento	Inexistente	Inicial	Definido	Procesando	Administrado	Optimizado
A5	Políticas de seguridad de la información	2					
A5.1.1	Las políticas de seguridad de la información	√					
A5.1.2	Revisión de las políticas de seguridad de la información	√					
A6	Organización de la seguridad de la información	5	1	1			
A6.1.1	Roles y responsabilidades en seguridad de la información	√					
A6.1.2	Segregación de tareas	√					
A6.1.3	Contacto con las autoridades	√					
A6.1.4	Contacto con grupos de interés especial	√					
A6.1.5	Seguridad de la información en la gestión de proyectos	√					
A6.2.1	Política de dispositivos móviles		√				
A6.2.2	Teletrabajo			√			
A7	Seguridad en el personal	6					

A7.1.1	Investigación de antecedentes	√					
A7.1.2	Términos y condiciones de contratación	√					
A7.2.1	Responsabilidades de gestión	√					
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	√					
A7.2.3	Proceso disciplinario	√					
A7.3.1	Responsabilidades de la finalización o cambio	√					
A8	Gestión de activos	6	3	1			
A8.1.1	Inventario de activos			√			
A8.1.2	Propiedad de los activos		√				
A8.1.3	Uso aceptable de los activos		√				
A8.1.4	Devolución de activos		√				
A8.2.1	Clasificación de la información	√					
A8.2.2	Etiquetado de la información	√					
A8.2.3	Manipulado de la información	√					
A8.3.1	Gestión de soportes extraíbles	√					
A8.3.2	Eliminación de soportes	√					
A8.3.3	Soportes físicos en tránsito	√					

A9	Control de acceso	5	3	3	1	2	
A9.1.1	Política de control de acceso					√	
A9.1.2	Acceso a las redes y servicios de red	√					
A9.2.1	Registro y baja de usuario			√			
A9.2.2	Provisión de acceso de usuario			√			
A9.2.3	Gestión de privilegios		√				
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	√					
A9.2.5	Revisión de los derechos de acceso de usuario	√					
A9.2.6	Retirada de los derechos de acceso	√					
A9.3.1	Uso de la información secreta de autenticación	√					
A9.4.1	Restricción del acceso a la información				√		
A9.4.2	Procedimientos seguros de inicio de sesión			√			
A9.4.3	Sistema de gestión de contraseñas		√				
A9.4.4	Uso de las utilidades con privilegios del sistema		√				

A9.4.5	Control de acceso al código fuente de los programas					√	
A10	Criptografía				2		
A10.1.1	Política de uso de los controles criptográficos				√		
A10.1.2	Gestión de claves				√		
A11	Seguridad física y del entorno	4	2	3	2	4	
A11.1.1	Perímetro de seguridad física					√	
A11.1.2	Controles físicos de entrada				√		
A11.1.3	Seguridad de oficinas, despachos y recursos					√	
A11.1.4	Protección contra las amenazas externas y ambientales			√			
A11.1.5	El trabajo en áreas seguras					√	
A11.1.6	Áreas de carga y descarga					√	
A11.2.1	Emplazamiento y protección de equipos				√		
A11.2.2	Instalaciones de suministro			√			
A11.2.3	Seguridad del cableado			√			
A11.2.4	Mantenimiento de los equipos		√				
A11.2.5	Retirada de materiales		√				

	propiedad de la empresa						
A11.2.6	Seguridad de los equipos fuera de las instalaciones	√					
A11.2.7	Reutilización o eliminación segura de equipos	√					
A11.2.8	Equipo de usuario desatendido	√					
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	√					
A12	Seguridad de las operaciones	3	1	2	2	4	2
A12.1.1	Documentación de procedimientos de operación					√	
A12.1.2	Gestión de cambios				√		
A12.1.3	Gestión de capacidades			√			
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	√					
A12.2.1	Controles contra el código malicioso					√	
A12.3.1	Copias de seguridad de la información				√		
A12.4.1	Registro de eventos						√
A12.4.2	Protección de la información del registro					√	

A12.4.3	Registros de administración y operación					√	
A12.4.4	Sincronización del reloj						√
A12.5.1	Instalación del software en explotación		√				
A12.6.1	Gestión de las vulnerabilidades técnicas	√					
A12.6.2	Restricción en la instalación de software	√					
A12.7.1	Controles de auditoría de sistemas de información			√			
A13	Seguridad de las comunicaciones	1		1	1	4	
A13.1.1	Controles de red				√		
A13.1.2	Seguridad de los servicios de red			√			
A13.1.3	Segregación en redes					√	
A13.2.1	Políticas y procedimientos de intercambio de información					√	
A13.2.2	Acuerdos de intercambio de información					√	
A13.2.3	Mensajería electrónica					√	
A13.2.4	Acuerdos de confidencialidad	√					
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	1		1	7	4	

A14.1.1	Requisitos y especificaciones de seguridad de la información	√					
A14.1.2	Seguridad de los servicios de aplicaciones en redes públicas					√	
A14.1.3	Protección de las transacciones de servicios de aplicaciones				√		
A14.2.1	Política de desarrollo seguro					√	
A14.2.2	Procedimiento de control de cambios en sistemas				√		
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo				√		
A14.2.4	Restricciones a los cambios en los paquetes de software			√			
A14.2.5	Principios de ingeniería de sistemas seguros					√	
A14.2.6	Entorno de desarrollo seguro					√	
A14.2.7	Externalización del desarrollo de software				√		
A14.2.8	Pruebas funcionales de seguridad de sistemas				√		
A14.2.9	Pruebas de aceptación de sistemas				√		

A14.3.1	Protección de los datos de prueba				√		
A15	Relación con proveedores	1	1	1	2		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores		√				
A15.1.2	Requisitos de seguridad en contratos con terceros				√		
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones			√			
A15.2.1	Control y revisión de la provisión de servicios del proveedor				√		
A15.2.2	Gestión de cambios en los servicios prestados por terceros	√					
A16	Gestión de incidentes de seguridad de la información	7					
A16.1.1	Responsabilidades y procedimientos	√					
A16.1.2	Notificación de los eventos de seguridad de la información	√					
A16.1.3	Notificación de puntos	√					

	débiles de la seguridad						
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	√					
A16.1.5	Respuesta a incidentes de seguridad de la información	√					
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	√					
A16.1.7	Recopilación de evidencias	√					
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	1	3				
A17.1.1	Planificación de la continuidad de la seguridad de la información		√				
A17.1.2	Implementar la continuidad de la seguridad de la información		√				
A17.1.3	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio		√				
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	√					

A18	Cumplimiento	4	2	2			
A18.1.1	Identificación de la legislación aplicable		√				
A18.1.2	Derechos de Propiedad Intelectual (DPI)			√			
A18.1.3	Protección de los registros de la organización			√			
A18.1.4	Protección de datos y privacidad de la información de carácter personal		√				
A18.1.5	Regulación de los controles criptográficos	√					
A18.2.1	Revisión independiente de la seguridad de la información	√					
A18.2.2	Cumplimiento de las políticas y normas de seguridad	√					
A18.2.3	Comprobación del cumplimiento técnico	√					
Suma	Una suma de los puntos	46	16	15	17	18	2

Resultados de los controles de ISO 27001 después del proyecto

N.º	Cumplimiento	Inexistente	Inicial	Definido	Procesando	Administrado	Optimizado
A5	Políticas de seguridad de la información				1	1	
A5.1.1	Las políticas de seguridad de la información					√	

A5.1.2	Revisión de las políticas de seguridad de la información				√		
A6	Organización de la seguridad de la información	1	1		1	2	2
A6.1.1	Roles y responsabilidades en seguridad de la información						√
A6.1.2	Segregación de tareas					√	
A6.1.3	Contacto con las autoridades		√				
A6.1.4	Contacto con grupos de interés especial	√					
A6.1.5	Seguridad de la información en la gestión de proyectos				√		
A6.2.1	Política de dispositivos móviles						√
A6.2.2	Teletrabajo					√	
A7	Seguridad en el personal				1	4	1
A7.1.1	Investigación de antecedentes					√	
A7.1.2	Términos y condiciones de contratación					√	
A7.2.1	Responsabilidades de gestión				√		
A7.2.2	Concienciación, educación y capacitación en seguridad de la información					√	

A7.2.3	Proceso disciplinario					√	
A7.3.1	Responsabilidades de la finalización o cambio						√
A8	Gestión de activos				1	3	6
A8.1.1	Inventario de activos						√
A8.1.2	Propiedad de los activos						√
A8.1.3	Uso aceptable de los activos					√	
A8.1.4	Devolución de activos						√
A8.2.1	Clasificación de la información						√
A8.2.2	Etiquetado de la información						√
A8.2.3	Manipulado de la información					√	
A8.3.1	Gestión de soportes extraíbles						√
A8.3.2	Eliminación de soportes					√	
A8.3.3	Soportes físicos en tránsito				√		
A9	Control de acceso		1	1	2	4	6
A9.1.1	Política de control de acceso						√
A9.1.2	Acceso a las redes y servicios de red			√			
A9.2.1	Registro y baja de usuario						√

A9.2.2	Provisión de acceso de usuario					√	
A9.2.3	Gestión de privilegios					√	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios				√		
A9.2.5	Revisión de los derechos de acceso de usuario					√	
A9.2.6	Retirada de los derechos de acceso						√
A9.3.1	Uso de la información secreta de autenticación				√		
A9.4.1	Restricción del acceso a la información						√
A9.4.2	Procedimientos seguros de inicio de sesión						√
A9.4.3	Sistema de gestión de contraseñas						√
A9.4.4	Uso de las utilidades con privilegios del sistema		√				
A9.4.5	Control de acceso al código fuente de los programas					√	
A10	Criptografía				2		
A10.1.1	Política de uso de los controles criptográficos				√		
A10.1.2	Gestión de claves				√		

A11	Seguridad física y del entorno		1	1		5	8
A11.1.1	Perímetro de seguridad física						√
A11.1.2	Controles físicos de entrada						√
A11.1.3	Seguridad de oficinas, despachos y recursos						√
A11.1.4	Protección contra las amenazas externas y ambientales					√	
A11.1.5	El trabajo en áreas seguras						√
A11.1.6	Áreas de carga y descarga						√
A11.2.1	Emplazamiento y protección de equipos					√	
A11.2.2	Instalaciones de suministro					√	
A11.2.3	Seguridad del cableado			√			
A11.2.4	Mantenimiento de los equipos		√				
A11.2.5	Retirada de materiales propiedad de la empresa						√
A11.2.6	Seguridad de los equipos fuera de las instalaciones					√	
A11.2.7	Reutilización o eliminación segura de equipos					√	

A11.2.8	Equipo de usuario desatendido						√
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia						√
A12	Seguridad de las operaciones		1			7	6
A12.1.1	Documentación de procedimientos de operación					√	
A12.1.2	Gestión de cambios					√	
A12.1.3	Gestión de capacidades						√
A12.1.4	Separación de los recursos de desarrollo, prueba y operación		√				
A12.2.1	Controles contra el código malicioso					√	
A12.3.1	Copias de seguridad de la información						√
A12.4.1	Registro de eventos						√
A12.4.2	Protección de la información del registro					√	
A12.4.3	Registros de administración y operación					√	
A12.4.4	Sincronización del reloj						√
A12.5.1	Instalación del software en explotación					√	
A12.6.1	Gestión de las vulnerabilidades técnicas						√

A12.6.2	Restricción en la instalación de software						√
A12.7.1	Controles de auditoría de sistemas de información					√	
A13	Seguridad de las comunicaciones					7	
A13.1.1	Controles de red					√	
A13.1.2	Seguridad de los servicios de red					√	
A13.1.3	Segregación en redes					√	
A13.2.1	Políticas y procedimientos de intercambio de información					√	
A13.2.2	Acuerdos de intercambio de información					√	
A13.2.3	Mensajería electrónica					√	
A13.2.4	Acuerdos de confidencialidad					√	
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información				1	7	5
A14.1.1	Requisitos y especificaciones de seguridad de la información					√	
A14.1.2	Seguridad de los servicios de aplicaciones en redes públicas					√	
A14.1.3	Protección de las transacciones de servicios de aplicaciones				√		

A14.2.1	Política de desarrollo seguro					√	
A14.2.2	Procedimiento de control de cambios en sistemas						√
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo						√
A14.2.4	Restricciones a los cambios en los paquetes de software					√	
A14.2.5	Principios de ingeniería de sistemas seguros					√	
A14.2.6	Entorno de desarrollo seguro					√	
A14.2.7	Externalización del desarrollo de software					√	
A14.2.8	Pruebas funcionales de seguridad de sistemas						√
A14.2.9	Pruebas de aceptación de sistemas						√
A14.3.1	Protección de los datos de prueba						√
A15	Relación con proveedores	1		1	1	2	
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores					√	

A15.1.2	Requisitos de seguridad en contratos con terceros					√	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones			√			
A15.2.1	Control y revisión de la provisión de servicios del proveedor				√		
A15.2.2	Gestión de cambios en los servicios prestados por terceros	√					
A16	Gestión de incidentes de seguridad de la información				1	1	5
A16.1.1	Responsabilidades y procedimientos						√
A16.1.2	Notificación de los eventos de seguridad de la información						√
A16.1.3	Notificación de puntos débiles de la seguridad				√		
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información					√	
A16.1.5	Respuesta a incidentes de seguridad de la información						√

A16.1.6	Aprendizaje de los incidentes de seguridad de la información						√
A16.1.7	Recopilación de evidencias						√
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio					1	3
A17.1.1	Planificación de la continuidad de la seguridad de la información						√
A17.1.2	Implementar la continuidad de la seguridad de la información						√
A17.1.3	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio					√	
A17.2.1	Disponibilidad de los recursos de tratamiento de la información						√
A18	Cumplimiento			1	2	2	3
A18.1.1	Identificación de la legislación aplicable						√
A18.1.2	Derechos de Propiedad Intelectual (DPI)						√
A18.1.3	Protección de los registros de la organización						√

A18.1.4	Protección de datos y privacidad de la información de carácter personal				√		
A18.1.5	Regulación de los controles criptográficos					√	
A18.2.1	Revisión independiente de la seguridad de la información				√		
A18.2.2	Cumplimiento de las políticas y normas de seguridad					√	
A18.2.3	Comprobación del cumplimiento técnico			√			
Suma	Una suma de los puntos	2	4	4	13	46	45