1.a.02 - Esbozo de un Plan director de seguridad

Grupo 4.

Álvaro Pérez Rey.
Daniel Sánchez Gómez.
Ignacio Aragón Polo.
Jesús Sayago Mey.
Maria Dolores Galán Tajero.

Incidentes de ciberseguridad.

9/11/2022

ÍNDICE

1- Introducción

1.1- Importancia de la seguridad de la información

Las empresas deben ser conscientes de la importancia que tiene para su negocio el manejo de información. Proteger la información de una empresa consiste en poner barreras de protección para bloquear posibles ataques, para esto es necesario diseñar un SGSI para su aplicación en la empresa bajo la norma ISO 27001 que permite obtener una visión global del estado de los sistemas de información y definen las medidas de seguridad a aplicar para prevenir incidentes.

1.2- Implementación de SGSI

La implementación de un sistema de gestión de la seguridad de la información (SGSI), es una opción fundamental cuando se trata de proteger la información ya que este tiene como objetivo principal proteger dicho activo a través de controles de seguridad que deben ser aplicados en la empresa.

Algunos de los beneficios de implantar un SGSI basado en la ISO 27001 pueden ser:

- Aumentar la confiabilidad de los servicios ofrecidos a los clientes de la empresa.
- Aumentar el prestigio de la empresa en el sector.
- Potenciar la aplicación de mejores prácticas de seguridad de la información.
- Protección de uno de los activos más importantes a nivel de organización como es la información.

La norma ISO 27002 es un estándar para la seguridad de la información y esta proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como la preservación de la confidencialidad, integridad y disponibilidad.

1.3- Plan Director de Seguridad

Un Plan Director de Seguridad consiste en la definición, priorización e implementación de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta una empresa hasta unos niveles aceptables.

Es fundamental para la realización del mismo que se alinee con los objetivos estratégicos de la empresa y que se defina un alcance e incorporación de las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la empresa o terceros que colaboren con ella.

Uno de los perfiles más importantes en la implantación de un SGSI es el responsable de la información. Este debe formar parte de la empresa de manera interna ya que asumimos que el SGSI afecta a la gestión del negocio de la empresa y que además todas las acciones futuras y decisiones solo puedan ser desarrolladas por la alta dirección de la organización.

Algunas de las funciones que llevará a cabo el responsable de seguridad será:

- Garantizar el cumplimiento de planes y objetivos de SGSI
- Informar a la empresa de la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad marcada.
- Determinar todos los criterios de aceptación de riesgos y sus correspondientes niveles.

2- Situación actual de la empresa

2.1- Contexto de la empresa, estrategia de negocio

La empresa, actualmente, es una empresa que se encarga de asesorar a autónomos y pymes a través de internet mediante, mayoritariamente, su página web. Actualmente se encuentra en pleno proceso estratégico de transformación digital para así extenderse.

Por lo tanto, la estrategia de negocio principalmente pasa por su página web ya que sin ella los servicios básicos y vitales de la empresa se verían afectados y estos colapsarían totalmente el flujo de trabajo de la organización.

2.2- Acotar y establecer un alcance

En este plan director de seguridad vamos a centrarnos en el departamento de IT, el cual consideramos que posee una mayor responsabilidad, según la estrategia de negocio que sigue la empresa, en materia de información y tecnologías ya que el plan inmediato de la empresa es digitalizarse en todos los ámbitos posibles.

Dentro de nuestro alcance establecido vamos a tener en cuenta:

- Sistemas y equipos.
- Personal.
- Aplicaciones necesarias para la digitalización y centralización de los datos.

2.3 - Identificación de los responsables de la gestión de los activos

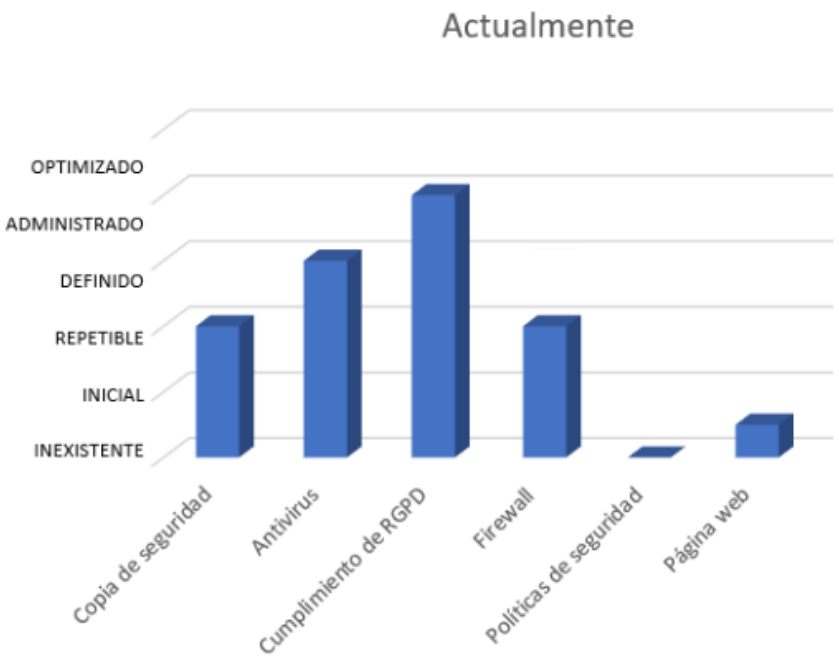
Es importante definir las responsabilidades sobre los activos de la empresa ya que estos son el bien más preciado que tiene y además nos facilitará hacer un seguimiento de las iniciativas implantadas. Estas responsabilidades deben estar asociadas a perfiles específicos.
Actualmente la empresa solo posee un responsable de seguridad, ya que el antivirus y el servidor de la página web están externalizados, el cual solo se encarga de la coordinación de las subcontratas de seguridad de ambas sedes.

Estudiando el departamento en el que nos hemos centrado confiamos en que una modificación de las distintas responsabilidades en seguridad de la información facilitará el seguimiento de la ejecución de las iniciativas que más tarde se vayan a implementar.

Un breve resumen de las diferentes responsabilidades sería el siguiente:

- **Responsable de seguridad**: Este responsable de seguridad estaría conformado por el responsable del departamento de IT y el departamento legal, este último será vital ya que necesitaremos conocimientos sobre las leyes que implican la protección de los datos.
- **Responsable de la información**: Se encargará de las responsabilidades asociadas al manejo de los datos. Este grupo de personas está conformado por el siguiente grupo de responsables, estos han sido elegidos ya que son los que manejan más información, o información más sensible de la empresa:
    - Facturación y ventas.
    - Compras.
    - Legal.
    - Consejo de administración.

2.4- Modelo de madurez



Copia de seguridad: Tienen documentado el proceso para que se repita tal y como viene en el documento.
Antivirus: Está documentado y gestionado por una subcontrata pero dirección aún no ha aprobado su implementación.
Cumplimiento de RGPD: Está todo documentado, aprobado y formal, todo administrado por una subcontrata.
Firewall: El procedimiento sólo lo conoce una persona.
Políticas de seguridad: No existen políticas por escrito.
Página web: No tenemos control de su securización ya que está externalizado.

2.5- Análisis de riesgos

2.5.1- Alcance del análisis

El área que vamos a analizar de la empresa es del departamento de TIC, ya que el mal funcionamiento o gestión de éste, puede afectar a las actividades de la empresa a nivel comercial y a la operativa interna y externa, así como, el tratamiento de la información de clientes, personal y servicios.

2.5.2- Análisis de los activos

Expondremos los activos más relevantes, físicos y lógicos que tiene la empresa. También respecto a los activos más importantes se expondrá la criticidad de dichos activos, denominándo cada uno por la gravedad: Baja, Media o Alta.

Los activos listados a continuación serán aquellos que hemos interpretado como vitales para el correcto funcionamiento de la empresa por lo que un mal uso de los equipos, una caída del servidor, o un ataque directo a estos activos sería fatal para la disponibilidad de las funciones principales de la empresa.

Activos	Descripción	Criticidad
Puestos de trabajo	PC, impresoras y teléfonos.	Medio
Dispositivos móviles	Portátiles, móviles y tabletas.	Bajo
Sistemas de almacenamiento	Discos duros y pendrive.	Alto
Servidores de la empresa	Serv. correo, archivos y aplicaciones.	Alto
Conexiones a internet	Routers y Wifi.	Alto
Datos e información de la empresa	Datos de clientes, proveedores, funcionamiento y gestión de la empresa	Alto
Propiedad intelectual	Creaciones de la empresa.	Bajo
Procesos en aplicaciones	Procesos internos en aplicaciones como CRM y ERP	Medio
Datos e información en la nube o servidor	Datos e información almacenados en la nube o en los servidores.	Alto
Aplicaciones en la nube	Aplicaciones almacenadas en servidores en la nube.	Medio

2.5.3- Análisis de las amenazas

Estas son todas las amenazas que tienen los activos y por los que pueden ser vulnerados. Más tarde indicaremos las vulnerabilidades de cada activo, causadas por las diferentes amenazas.

En primer lugar, antes de exponer las amenazas de mayor gravedad, se mostrarán las amenazas que se asumirán a causa de su bajo riesgo o probabilidad.

Amenazas asumibles:

- Daños por fuego, agua o desastres naturales.
- Degradación de los soportes de almacenamiento.

Amenazas
Respecto a la información: fuga, destrucción, alteración, corrupción e intercepción.
Errores de usuario, administrador y configuración.
Fallo de suministro eléctrico, comunicación, temperatura y servicios esenciales
Errores de mantenimiento de software y hardware.
Acceso no autorizado por abuso de privilegios.
Difusión de malware.
Robo, extorsión e ingeniería social.
Denegación de los servicios.

2.5.4- Establecimiento de las Vulnerabilidades

Exposición de cada una de las vulnerabilidades relacionadas con sus correspondientes activos.

Hemos elegido estos activos al ser los que mayor criticidad tienen, para así dar prioridad y centrarnos en los activos y vulnerabilidades más importantes.

Activos	Vulnerabilidades
Sistemas de almacenamiento: Discos duros.	• No tener un protocolo de encriptación de los discos duros ante el robo de la información. • No tener un protocolo de comprobación de la integridad de los sistemas de almacenamiento.
Datos e información almacenada de la empresa: clientes, proveedores, funcionamiento y gestión de la empresa.	• No tener una política por escrito de destrucción de datos, informes y soportes. • Tener una mala gestión de los datos o información de la empresa.
Servidores de la empresa: Serv. correo, archivos y aplicaciones.	• No tener todos los servidores centralizados. • No tener una seguridad física en las instalaciones del CPD. • No tener protocolos de acción ante catástrofes en los servidores. • No tener un controlador de temperatura y de humedad en el CPD central. • La inadecuada gestión de cuentas y contraseñas.
Conexiones a internet: Routers y Wifi.	• No tener herramientas de monitoreo de red ante ataques. • Protocolos de cifrado de la información que se transmite por la red de la empresa. • La inadecuada gestión de cuentas y contraseñas.

2.5.5- Evaluación y cálculo de riesgo

En este punto identificamos y evaluamos el cálculo del riesgo con respecto a los activos-amenazas que tiene la empresa.

Para esto se emplearán dos métodos de tratamiento del riesgo, una será la aceptación del riesgo en cuestión al no tener un porcentaje de riesgo significativo para el funcionamiento de la empresa. Por otro lado, el segundo método consistiría en tener en cuenta dicho riesgo y crear políticas o soluciones para solventar dichas amenazas.

- Amenazas-Activos a tener en cuenta:

  Tomaremos éstas, como las Amenazas-Activos más relevantes e importantes para la empresa.

Amenaza	Activos
Fuga/Alteración/Destrucciones de información	Ordenadores/Servidores, Página Web/Tienda online y RRHH, Herramientas en la nube, Herramientas para la administración en la nube.
Difusión de software dañino	Ordenadores/Servidores, Dispositivos móviles, Herramientas comerciales, Pagina Web/Tienda online y RRHH, Herramientas en la nube
Denegación de servicio y caída de los servicios	Página Web/Tienda online y RRHH, Herramientas en la nube.
Acceso no autorizado	Ordenadores/Servidores, Conexión a internet con wifi, Herramientas para la administración online.
Robo	Dispositivos móviles, página web/tienda online y RRHH.

- Amenazas-Activos a asumir:

  Algunos ejemplos de las Amenazas-Activos que la empresa asumirá, al no tener tanta relevancia para el funcionamiento de los servicios de la empresa, son los siguientes:

Amenaza	Activos
Daños por fuego, agua o desastres naturales.	Serv. correo, archivos y aplicaciones
Degradación de los soportes de almacenamiento.	Serv. correo, archivos y aplicaciones.
Errores de comunicación, de administración y de mantenimiento.	Aplicaciones almacenadas en servidores en la nube.
Errores de mantenimiento, fallo de los servicios de comunicación.	Procesos internos en aplicaciones como CRM y ERP.
Errores de administración y de usuarios	Dispositivos móviles con datos y apps para el trabajo.

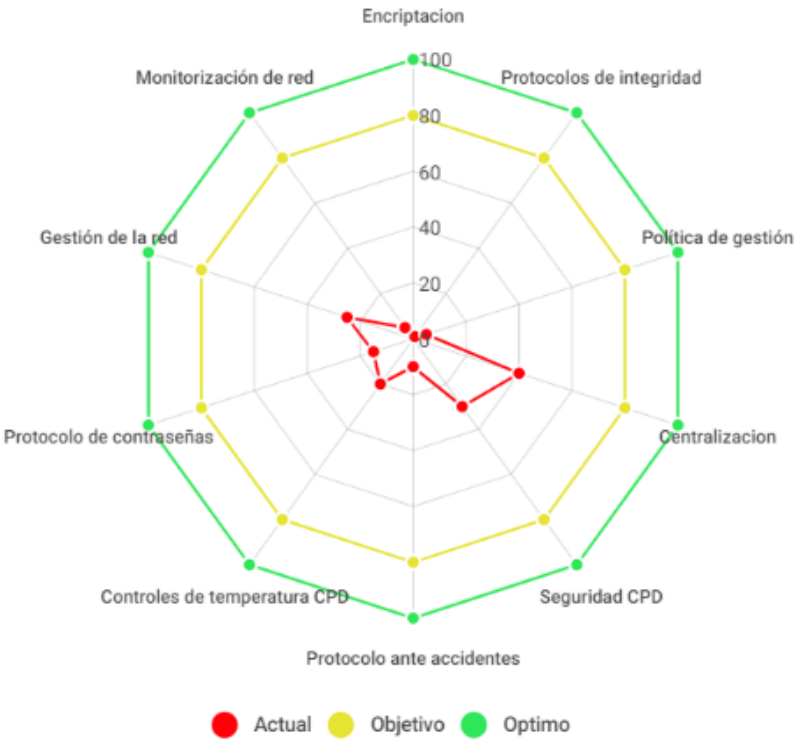
2.6- Objetivos basados en los activos críticos

A continuación en este apartado se expondrá una gráfica en la cual veremos diferentes niveles:

- El nivel óptimo que debería tener la empresa en cuanto a medidas de seguridad.
- El objetivo propuesto, para que la empresa funcione correctamente.
- El nivel de madurez que tiene la empresa actualmente con respecto a las vulnerabilidades de los activos críticos, especificados anteriormente.

Tenemos en la gráfica los diferentes procesos vitales, de los cuales se crearán los proyectos para cada una de las vulnerabilidades de los activos críticos. Los puntos a tratar de los cuales se crearán los proyectos son los siguientes:

- Encriptación.
- Monitorización de red.
- Protocolos de integridad de la información.
- Políticas de gestión.
- Centralización
- Seguridad de CPD.
- Protocolos ante accidentes.
- Controles de temperatura y humedad en el CPD.
- Protocolos/Políticas de contraseñas.
- Gestión de la red.



3- Estrategia de la empresa

Ya que la empresa se dedica principalmente a asesorar a autónomos y pymes, su principal método para captar clientes es mediante una página web/ tienda online, además utilizan las redes sociales para darse a conocer y mostrar todos los servicios que ofrecen. Por esto, la empresa sigue actualmente un plan estratégico de transformación digital para extenderse y realizar la mayoría de trabajos a través de internet mediante su página web.

Por lo que una vez hemos averiguado cual es la estrategía de la empresa y viendo el carácter propio que sigue, vemos que tanto el servidor de la página web como la seguridad física en la primera y segunda sede están externalizadas.

En conclusión, vemos que algunos importantes servicios que tiene esta empresa están externalizados y esto puede llegar a causar graves problemas de seguridad, así que para el correcto desarrollo de las actividades vitales de la empresa crearemos unos proyectos e iniciativas, en materia de seguridad de la información y siempre a la par con la filosofía de la empresa y los responsables de los diferentes departamentos, para prevenir este tipo de incidentes.

4- Definición de proyectos e iniciativas

A partir de la información recabada, definiremos las acciones, iniciativas y proyectos necesarios para implementar las salvaguardas necesarias para el tratamiento de los riesgos identificados en el proceso de análisis de riesgos y así alcanzar el nivel de seguridad adaptada a las necesidades de la empresa. Tomaremos como referencia el código de prácticas para los controles de seguridad de la información de la norma UNE-ISO/IEC 27002.

ID	PROYECTO	DESCRIPCIÓN	PUNTOS DE CONTROL
01	Desarrollar e implementar una política de seguridad.	Desarrollar e implementar una política de seguridad que contenga al menos los siguientes aspectos: -Compromiso de la Dirección. -Utilización del e-mail e Internet. -Utilización de dispositivos móviles, unidades de almacenamiento externo . -Aspectos de protección de datos.	5.1.1 Conjunto de políticas para la seguridad de la información. 6.2.1 Política de uso de dispositivos para movilidad.
02	Desplegar un plan de concienciación en materia de seguridad de la información.	Crear un programa de formación y concienciación que cubran tanto el personal de los departamentos operativos como la Dirección.	7.2.2 Concienciación, educación y capacitación en la seguridad de la información.

03	Clasificación de la información (Pública, privada y confidencial) y su tratamiento.	Desarrollar una política de tratamiento de la información que gestiona la empresa. Desarrollar una política de destrucción de datos, informes y soportes.	18.1.3 Protección de los registros. 18.1.4 Protección de los datos y la privacidad de la información personal.
04	Política de copias de seguridad.	Analizar la información corporativa y crear e implantar una política de copias adecuada, la encriptación y la verificación de su integridad.	12.3.1 Copias de seguridad de la información. 10.1.1 Política de usos de los controles criptográficos.
05	Regulación de los servicios TIC prestados por terceros.	Revisar los contratos establecidos con los proveedores TIC externos para garantizar que estos son adecuados a las necesidades de la organización. Para aquellos que sean críticos, establecer acuerdos de nivel de servicio.	15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros.
06	Política de Seguridad de la Red Corporativa.	Desarrollar y documentar el hardening de los sistemas de la red de la empresa. (Servidores, firewall). Centralización de los sistemas.	11.2.4 Mantenimiento de equipos 13.1.3 Segregación de redes.
07	Política de seguridad física del CPD	Implementar controles físicos de entrada, amenazas externas y ambientales	11.2.1 Controles físicos de entrada. 11.1.4 Protección contra las amenazas externas y ambientales. 12.2.1 Emplazamiento y protección de equipos.
08	Política de Control de Accesos	Desarrollar un protocolo de control de accesos, revisar los servicios prestados por terceros y adecuarlos a las necesidades de la empresa. Implementación de Política de Autenticación de usuarios.	9.1.1 Política de control de accesos.

09	Política de administración de cuentas y contraseñas.	Desarrollar directrices y procedimientos que permitan diseñar las pautas para el control de acceso, modificación, y eliminación de cuentas por parte de los administradores. Implantación de un sistema de gestión de contraseñas.	9.2 Gestión de acceso de usuarios. 9.4.3 Gestión de contraseñas de usuario.
10	Adquirir servicios de monitoreo SOC	Implementar y configurar sistemas de monitoreo para prevenir ataques, analizar eventos y prevenir malware. Desarrollar procedimientos para la gestión de alertas y escalamiento de eventos e incidentes.	16.1.1 Responsabilidad y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.4 Respuesta a los incidentes de Seguridad. 16.1.7 Recopilación de evidencias.

5- Clasificación y priorización de los proyectos

Prioridad muy alta

	Responsable	Tipo	Coste
Política de copias de seguridad.	Información	Organizativa	765€
Política de seguridad física de CPD.	Seguridad	Organizativa	300€

Prioridad alta

	Responsable	Tipo	Coste
Desarrollar e implementar una política de seguridad.	Información	Organizativa	650€
Clasificación de la información y su tratamiento.	Información	Organizativa	250€

Regulación de los servicios TIC ofrecidos por terceros.	Seguridad	Técnica	300€
Política de seguridad de la red corporativa.	Seguridad	Técnica	800€
Política de control de accesos.	Seguridad	Técnica	400€
Servicios de monitoreo SOC.	Seguridad	Técnica	1200€

Prioridad media

	Responsable	Tipo	Coste
Plan de concienciación en materias de ciberseguridad.	Información	Organizativa	295€
Política de administración de cuentas y contraseñas.	Seguridad	Organizativa	350€

Gráfica por precios de los proyectos clasificados y priorizados

6- Aprobación del PDS

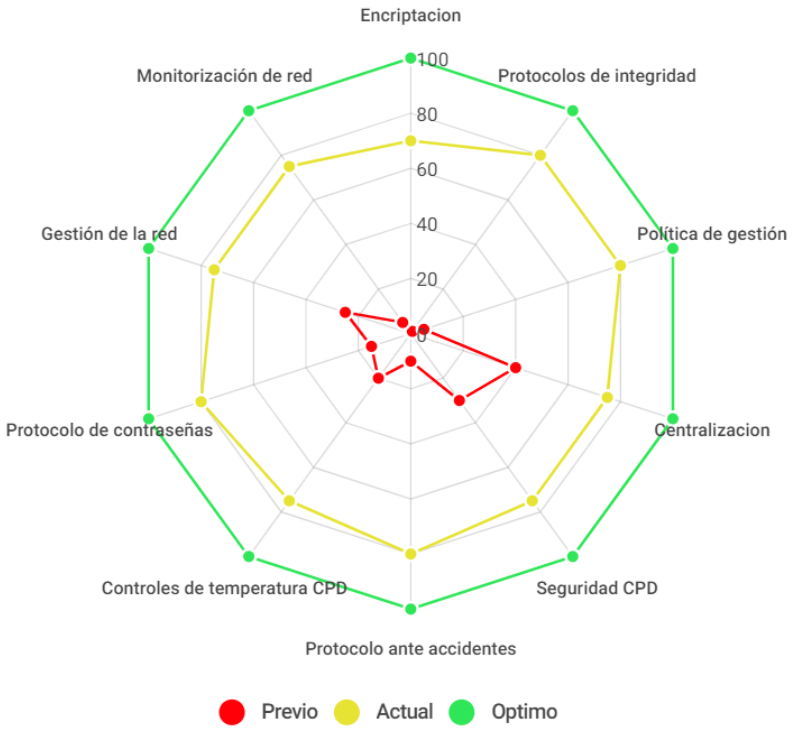
Una vez llegados a este punto dispondremos una versión preliminar de nuestro PDS, por lo que es el momento de revisarlo y mostrárselo a la dirección de la empresa para que así nos den su visto bueno.

En el caso de que haya que modificar algún criterio como el alcance, duración o prioridad de algunos proyectos el proceso de revisión se repetirá de manera cíclica hasta disponer de una versión final aprobada por la empresa.

Tras la revisión con la dirección de la empresa, se ha determinado que el planteamiento es correcto, a excepción de la priorización en el punto de las copias de seguridad, ya que de un primer enfoque en el que se consideraba que tenía una prioridad alta, la dirección de la empresa ha considerado que la política aplicada para las copias de seguridad es un elemento dentro del plan de actuación con una prioridad muy alta.

La comunicación a los empleados se realizará vía circular, mediante correo electrónico a la dirección asignada a cada empleado de la compañía.

A continuación mostraremos el gráfico de la madurez de la seguridad en la empresa una vez se han implementado y aplicado los diferentes proyectos e iniciativas que forman parte de este plan director de seguridad.



7- Puesta en marcha del PDS

Una vez aprobado nuestro PDS comenzaremos a poner en marcha una serie de pasos que favorecen el éxito de cada de los proyectos presentados y, en consecuencia, el cumplimiento de los objetivos establecidos.

Para cada una de las iniciativas que vamos a implementar realizaremos una presentación general con las personas implicadas haciéndolas así partícipes e informándoles de los resultados que persiguen. En el caso de una iniciativa que implemente un control de seguridad, nos pondremos en contacto en primer lugar con el encargado de seguridad de nuestra empresa y los trabajadores que hemos contratado para que implementen esta medida.

Otro de los puntos importantes de la puesta en marcha del PDS es asignar los responsables o coordinadores de cada proyecto y dotarlo de las herramientas y recursos necesarios. Siguiendo la trazabilidad del proyecto comentado con anterioridad, para el proyecto que implementa controles de acceso, asignaremos un responsable o responsables, que serán el administrador de red en el caso del acceso remoto y el encargado de los guardias de seguridad en el caso del acceso físico al edificio. Destacar que ambos estarán apoyados por el responsable de seguridad de la empresa que será el encargado de llevar a cabo todo el PDS.

También debemos establecer una periodicidad con la que llevar a cabo el seguimiento individual de los proyectos así como el seguimiento conjunto del PDS.

Finalmente a medida que vayamos alcanzando los objetivos deberemos de confirmar que las deficiencias identificadas previamente han sido subsanadas.

8- Tareas asociadas y responsables

Responsable	Proyecto
Daniel Sánchez Gómez	Portada, Indice, 2.5, 2.6 y gráfica(p.6)
Álvaro Pérez Rey.	Índice, 1, 2.1, 3 y 7
Ignacio Aragón Polo.	4
Jesús Sayago Mey.	5 y 6
Maria Dolores Galán Tajero.	Resumir los puntos, 2.2, 2.3 y 2.4

9- Bibliografía

EjemploPlanDirectorDeSeguridad.pdf

Plan-director-seguridad.pdf

Plan director de seguridad.pdf

Control de ISO 27002.pdf

Control ISO 27002 Ampliado.pdf

Listado de Amenazas y Vulnerabilidades ISO27000.pdf

https://www.cronoshare.com/cuanto-cuesta/servicio-ciberseguridad-empresas

https://ayudaleyprotecciondatos.es/2020/10/30/plan-director-de-seguridad/#Ejemplos

https://docs.google.com/document/d/1lciAYQl5yNsi9GBxaLU4WSFZEAdPtDMK/edit