Incidentes de Ciberseguridad

Práctica 1.a.02 — Plan director de seguridad

— *Grupo 3*

Raúl Ladrón de Guevara García

Juan Manuel Cumbrera López

Christian Romero Oliva

Sergio Guerrero Merlo

Índice

1. Introducción

El Plan Director de Seguridad constituye un documento esencial a la hora de sentar las bases para proteger los activos críticos de la compañía, así como salvaguardar la integridad de la información en la organización, dado que este establece los objetivos, las estrategias y las medidas necesarias para proteger dichos activos.

Dada la importancia de adaptarse a un mundo cambiante totalmente interconectado y sujeto a múltiples amenazas, el PDS resulta ser completamente necesario, erigiéndose como la estrategia a seguir por la empresa.

1.1 Importancia de la seguridad de la información

Las modernas tecnologías de la información han ido convirtiéndose de forma progresiva en un aspecto clave de las vidas de millones de personas, tanto a nivel recreativo como laboral. A medida que estas se hacían más y más presentes en el mundo que nos rodea, se ha ido haciendo evidente el hecho de que se han tornado irremplazables y absolutamente necesarias.

En la actualidad casi todas las empresas, desde las más grandes hasta incluso muchas pequeñas, dependen de estas tecnologías. Algunas incluso dependen tanto de la tecnología como para desarrollar en gran medida su trabajo haciendo uso de sistemas informáticos, lo que lleva a la necesidad de implementar medidas de seguridad que permitan mantener la información a salvo, lejos de delincuentes y oportunistas que pudieran o tratarán de acceder a ella de forma no autorizada.

Por todo esto, es de crucial importancia que las empresas dispongan de un Plan Director de Seguridad bien estructurado y eficiente, que permita reducir los riesgos de forma efectiva.

1.2 Plan Director de Seguridad

El plan Director de Seguridad desarrollado consta de un conjunto de proyectos diseñados para reducir los riesgos a los que la empresa está sometida, de modo que dicha cantidad pueda ser considerada como aceptable. Para lograr esto se debe partir de un análisis adecuado del estado general de la compañía, a fin de poder desarrollar el susodicho plan correctamente.

El plan debe estar en línea con la estrategia de la empresa e incluir las responsabilidades y las mejores prácticas que los empleados deben seguir. En caso de alcanzar un nivel de madurez adecuado, podríamos considerar la certificación de nuestro sistema de gestión de seguridad de la información.

El objetivo último de este plan director de seguridad es planificar los proyectos que se llevarán a cabo a nivel técnico, organizativo y legal, a fin de garantizar la seguridad de la información de nuestra empresa, alineándose con los intereses estratégicos de la empresa, tal y como se ha mencionado con anterioridad.

2. Situación Actual de la Empresa

En la actualidad la empresa dispone de controles de seguridad básicos, lo que supondría pocos problemas para posibles atacantes a la hora de acceder ilegalmente a los servicios y sistemas de la compañía. Además de este principal problema, existen varios aspectos que deben ser revisados, a fin de mejorar la seguridad general de la empresa.

Uno de los puntos clave en los que nos enfocaremos será la seguridad digital, y para ello, después de un análisis de los activos de la empresa, observamos que disponen de una página web en un servidor alojada en un servidor de hosting remoto sobre el cual no tienen control. Consideramos que la empresa debería mantener un control sobre sus activos de forma directa, de modo que no dependa de terceros, o que lo haga en la mínima medida posible, y por ello alojar la página web en un servidor propio seguro y bajo control es una mejor opción.

No existen políticas de seguridad establecidas, sin embargo, se dispone de un procedimiento de seguridad relacionado con un antivirus instalado por un subcontratista, quien se encarga de gestionar sus actualizaciones. La compañía dispone también de un firewall que la divide en 2 secciones, una segura y otra pública, pero únicamente el administrador de red tiene conocimiento de las configuraciones de seguridad.

En cuanto a la seguridad física, la empresa dispone plan básico de copias de seguridad almacenadas en la sede principal, el cual está controlado por el equipo de seguridad. También tienen un equipo de seguridad externo contratado que se encarga de la seguridad de las 2 oficinas de las que disponen.

Las políticas y normativas de las que disponen son un RGPD (Reglamento General de Protección de Datos) que elaboró una consultoría, bastante bien documentado por lo

que lo dejaríamos en un plano más secundario. La subcontrata del antivirus elaboró un procedimiento escrito, pero no ha sido revisado por la dirección, por lo que es importante que se decida sobre él con prontitud. Es importante apuntar que no disponen de políticas de seguridad por escrito, lo que debería ser una de nuestras prioridades.

2.1 Contexto de la empresa y estrategia de negocio

Nuestra empresa actúa con el propósito de dar servicio de consultoría a *pymes* y autónomos a través de una página web, que además de ofrecer servicios de asesoramiento, permite que los clientes puedan contactar con la compañía a fin de proporcionar los trabajos.

Se ha desarrollado una estrategia de transformación digital para extenderse y llevar a cabo la mayoría de sus trabajos por internet, dependiendo de la página web y la tienda que contiene.

Además de todo lo anterior, la metodología seguida para dar a conocer la empresa ha consistido en el uso de las redes sociales, mostrando la cartera de servicios a través de estas.

2.2 Acotar y establecer un alcance

Después de una ardua investigación del contexto de la empresa y de su estrategia de negocio, definimos un acotamiento y un alcance de los activos que creemos más importantes para la empresa.

En base a esta investigación, hemos seleccionado una serie de activos que creemos que son críticos para la empresa ya que son activos que no deben caer en ningún momento al ser los pilares del funcionamiento del negocio de la empresa.

Todo activo que no consideramos críticos, estarán fuera de este plan de seguridad o por lo menos, serán dejados para un futuro.

Los activos críticos que hemos considerado son los siguientes:

- La sede principal.
- La segunda sede que está ubicada en una segunda planta de otro edificio ajeno a la sede principal.

- Los empleados de los departamentos como el de compras, el de ventas y facturación, el de comunicación y el de delivery.
- La página web y la tienda online.
- Las redes sociales donde la empresa se da a conocer y es uno de los pilares importantes dentro de la estrategia de digitalización de la empresa.
- El servidor de correo electrónico.
- El servidor de archivos y aplicaciones.
- Equipo informático de los jefes de departamento y del consejo de administración.
- Servicios en la nube.
- Propiedad intelectual.
- Consejo de administración.

Estos son los activos críticos que debemos considerar dentro de nuestra empresa para llevar a cabo proyectos para poder asegurarlos y mitigar posibles vulnerabilidades o directamente eliminar los riesgos sobre estos activos críticos.

2.3 Identificación de los responsables de la gestión de los activos

Se ha identificado una serie de responsables que gestionan los activos. Estos responsables son desde empleados que acceden a su puesto de trabajo, como los jefes de departamento y hasta un departamento al completo como es el caso del departamento de TIC que se encarga de gestionar los servidores que se encuentran alojados en nuestra empresa.

Los empleados de cada departamento son responsables de su puesto de trabajo y de los dispositivos informáticos o electrónicos que se encuentran en él o están a su cargo para poder ejercer su trabajo de manera correcta.

En estos activos se encuentran desde equipos informáticos como ordenadores, tablets hasta telefonía móvil.

Los servidores alojados en nuestra empresa están a cargo de los empleados del departamento TIC que se encargarán del tratamiento y mantenimiento de estos servidores.

El servidor web y por consiguiente la página y su tienda online están externalizadas, por ello los responsables de su seguridad es la empresa que tenemos contratada para que nos lleve este servicio.

El responsable de nuestras sedes será el jefe de la empresa ya que es el encargado de comprar o alquilar el edificio y la segunda sede en la segunda planta del edificio donde se encuentra. Igualmente la seguridad de ambas sedes estará a cargo de la empresa contratada para ello.

2.4 Análisis de riesgos

El análisis de riesgos constituye un componente fundamental en el plan director de seguridad,proporcionando evaluación integral de las amenazas y vulnerabilidades a las que una organización está expuesta. En esta sección exploraremos el alcance del análisis a llevar a cabo, el análisis de los activos de la empresa, de las amenazas, así como un establecimiento de las vulnerabilidades, y una evaluación y cálculo del riesgo, con el objetivo de garantizar la protección de activos críticos, la continuidad del negocio y la integridad de la información.

El análisis de riesgos se fundamenta como un pilar esencial en el diseño de un plan de seguridad efectivo, permitiendo a la organización tomar decisiones informadas para enfrentar los desafíos presentes y futuros en el ámbito de la seguridad.

2.4.1 Alcance del análisis

El alcance del análisis lo centraremos en los departamentos que a nuestro parecer son más críticos para la empresa. Estos departamentos son el departamento de facturación y ventas, el departamento de compras, el consejo de administración, el departamento de delivery y el departamento de comunicación y redes sociales. En estos departamentos se encuentran datos personales de clientes y proveedores, datos de gestión y el funcionamiento de la empresa, actividades comerciales, el servicio de atención al cliente, etc. Los demás departamentos los excluimos del análisis ya que no podemos abarcar todos y no nos parecen tan críticos como los mencionados.

2.4.2 Análisis de los activos

Tras analizar los distintos activos que tenemos en nuestra empresa, estos son los activos que consideramos más críticos:

- **Servidor web:** La mayoría de las ventas se realizan a través de la página web por lo que si esta falla afectaría al flujo de ingresos de la empresa.
- **Servidores de archivos y aplicaciones:** Si los servidores de archivos y aplicaciones fallan o sufren algún tipo de ataque supondría un grave problema para la empresa ya que se podría interrumpir el funcionamiento de la misma o perder datos de clientes y proveedores.
- **Los empleados:** Debido a que tienen acceso a datos sensibles de clientes y de la propia empresa y podrían realizar acciones maliciosas con estos datos o cometer errores dejando brechas de seguridad.
- **Software de gestión de relaciones con el cliente (CRM):** Si el CRM falla, se podría perder la capacidad de establecer relaciones con los clientes lo que afectaría a las ventas.
- **Servicios en la nube:** Si los servicios en la nube fallan o son hackeados esto podría suponer un gran problema para la empresa ya que en estos servicios se almacenan muchos datos de clientes y de la empresa por lo que la información podría perderse o quedar expuesta.
- **Propiedad intelectual:** La pérdida de marcas registradas, secretos comerciales, etc... podría tener un impacto en la capacidad de la empresa para mantener su posición en el mercado.
- **Tienda online:** Si la tienda online falla o sufre interrupciones, esto puede afectar al flujo de ingresos de la empresa ya que no se podrían realizar compras por parte de los clientes.
- **Comunicación y redes sociales:** La comunicación con los clientes a través de las redes sociales y otros medios es importante, si la comunicación con los clientes falla o se ve afectada, esto puede tener un impacto en la percepción del cliente sobre la empresa.
- **Servidor de correo:** El servidor de correos es importante para la comunicación interna y externa, si este falla o sufre interrupciones se puede ver afectada la productividad y la comunicación de la empresa.
- **Equipos Informáticos de la Junta Directiva y del Consejo de administración:** En estos equipos se encuentran los datos importantes de gestión y del funcionamiento de la empresa. Si esta información llegase a perderse, corromperse o sufrir un ataque informático, la empresa podría verse afectada gravemente.

2.4.3 Análisis de las amenazas

Para llevar a cabo un análisis de riesgos efectivo, es importante identificar las amenazas y vulnerabilidades que pueden afectar a los activos críticos mencionados anteriormente. Estas amenazas son:

- **Amenazas informáticas:** Ataques de hackers, malware, phishing, ransomware y otros tipos de ciberataques que podrían comprometer la seguridad de los servidores, la página web, los datos en la nube, etc...
- **Desastres naturales:** Eventos como incendios, inundaciones, terremotos, y otros desastres naturales que podrían dañar los servidores y los sistemas.
- **Errores humanos:** Fallos accidentales o acciones inapropiadas por parte de los empleados que podrían resultar en la pérdida de datos o la exposición de información confidencial.
- **Fallos de hardware y software:** Problemas técnicos que podrían afectar el funcionamiento de los sistemas, servidores y el software, lo que impactaría en el funcionamiento de la empresa.
- **Amenazas internas:** Acciones maliciosas por parte de empleados descontentos o personas con acceso interno que podrían comprometer la seguridad de los datos y los sistemas.
- **Cambios regulatorios:** Modificaciones en las regulaciones que podrían requerir ajustes en la forma en que la empresa trabaja por ejemplo con los datos de los clientes o con los procedimientos que tienen que seguir para vender los servicios, lo que podría afectar su funcionamiento y su flujo de ingresos.

2.4.4 Establecimiento de las vulnerabilidades

Las posibles vulnerabilidades que podrían tener nuestra empresa en relación con los activos y las amenazas que hemos descrito anteriormente son:

- **Dispositivos y software no actualizados:** Si no se realizan actualizaciones del software y los sistemas operativos se puede exponer la empresa a vulnerabilidades conocidas que los ciberdelincuentes pueden explotar.
- **Mala gestión de los accesos a datos y aplicaciones:** Una mala gestión de los accesos a los datos y aplicaciones puede llevar a la exposición de información confidencial a personas no autorizadas.
- **Falta de concienciación en los empleados:** La falta de concienciación en seguridad de los empleados puede dar lugar a acciones como la apertura de correos electrónicos de phishing.

- **No revisar las copias de seguridad:** Si no se revisan las copias de seguridad de los datos estas podrían no funcionar y perderse toda la información.
- **Usar contraseñas débiles:** Si se utilizan contraseñas débiles o la misma contraseña para varios servicios o aplicaciones de la empresa los ciberdelincuentes podrían realizar ataques de fuerza bruta y conseguir acceso a los mismos fácilmente.
- **Protección en los servidores:** No existe ningún tipo de protección en los servidores contra subidas de tensión o apagones por lo que estos podrían sufrir daños.

2.4.5 Evaluación y cálculo de riesgo

Es preciso disponer de una evaluación de los posibles riesgos que pueden tener nuestros activos más críticos de la empresa. Este riesgo viene dado por la probabilidad de que ocurra una amenaza que pueda vulnerar ese activo y el impacto que podría ocasionar no solo a la empresa como entidad y sus empleados si no también a nuestra estrategia de negocio.

Las amenazas pueden ser desde un error de un empleado de la propia empresa hasta factores que escapan de nuestro control como un corte de electricidad a través de una tormenta eléctrica.

Esta evaluación se ha tenido en cuenta parcialmente para planificar una serie de proyectos a implementar y varias iniciativas que llevar a cabo.

La página web y tienda online es un activo que puede ser accesible de manera pública y puede incitar a que cibercriminales intenten atacar de muchas maneras. Este tipo de ataques pueden ser de una probabilidad media dependiendo de los sistemas de seguridad de la empresa que tenemos contratada para este servicio pero el impacto es alto.

Los servidores pueden ser vulnerados de muchas maneras, desde cibercriminales hasta problemas con el control del entorno y el factor humano. La mayoría de las probabilidades de que ocurran estas amenazas pueden estar entre un valor medio y alto pero el impacto es de valor alto ya que son un activo importante para el negocio.

Los errores humanos son un problema grave para la empresa siendo de una probabilidad alta, dependiendo del error humano puede tener un impacto alto para nuestra empresa.

Los problemas con el software dependen de muchos factores, entre ellos errores de configuración por administradores del sistema o de las propias actualizaciones. La probabilidad de que esto ocurra puede ser baja con un impacto medio. Este impacto medio dependerá del software que sea susceptible a estas amenazas.

No solo el software debe ser evaluado dentro de esta evaluación de riesgos, los problemas con el hardware puede tener una probabilidad media de que ocurra dependiendo de la antigüedad de los equipos como del mantenimiento llevado a cabo. El impacto puede ser alto si el hardware hace referencia a los servidores y medio si es de un empleado en cuestión.

Cualquier riesgo pueda tener un valor de impacto alto deben de ser mitigados. Los valores medios que puedan ser eliminados o dado a un valor bajo, se tendrán en cuenta para proyectos a largo plazo. Serán prioritarios los proyectos que puedan mitigar los valores de impacto alto teniendo en cuenta los recursos financieros de la empresa.

2.5 Objetivos basados en los activos críticos

Hemos definido una serie de objetivos con el propósito de mejorar la protección de los activos más importantes de nuestra empresa, como pueden ser los datos, sistemas informáticos, la infraestructura física y la concienciación de los empleados.

Nuestros objetivos, centrados en los activos críticos de la empresa, son los siguientes:

- Aumentar la seguridad de los sistemas críticos de la empresa.
- Disponer de una plantilla de trabajadores formada y concienciada de los riesgos de seguridad existentes.
- Disponer de un plan de respuesta ante incidentes detallado para abordar y mitigar las amenazas e incidentes cuando ocurran.
- Controlar el acceso a los datos y sistemas de la empresa.
- Mejorar la seguridad física de los activos críticos.
- Aumentar la seguridad de las redes de la empresa.
- Tener el control total de la página web y la tienda online.
- Mantener la integridad de los datos revisando las copias de seguridad.

3. Estrategia de la Empresa

Se ha decidido que se seguirá una estrategia de transformación progresiva, a un ritmo mediano, con el objetivo de completar todas las iniciativas y proyectos en el plazo máximo de un año.

El concepto de la estrategia será el de *defensa en profundidad*, un plan enfocado a endurecer y añadir capas de seguridad a nuestros activos más críticos con el objetivo de ralentizar y entorpecer el avance de los posibles atacantes, así como contener y amortiguar los daños sufridos por otro tipos de amenazas como desastres naturales o ataques de ingeniería social.

Por supuesto debemos tener en cuenta que nuestra estrategia, aunque esté focalizada en un objetivo debe ser también muy flexible, debido a que el mundo de la ciberseguridad está en constante y rápida evolución. Los puntos más importantes para que la estrategia se pueda llevar a cabo son los siguientes:

- La estrategia en seguridad debe ser respaldada por los altos cargos de la empresa, garantizando que se confía en la importancia de la misma.
- Debe ser dirigida y controlada. El ritmo de cambio establecido no debe ser muy rápido, para no provocar que se efectúen cambios descuidados, ni muy lenta, para llevar a cabo el plan en un marco de tiempo útil.
- Se deben tomar decisiones en base a la información y hechos, no a suposiciones ni conjeturas.

Los plazos, iniciativas y proyectos que se llevarán a cabo conformes a esta estrategia serán descritos en los siguientes puntos.

4. Definición de Proyectos e Iniciativas

Definiremos una serie de proyectos e iniciativas que llevar a cabo para mitigar un conjunto de posibles riesgos para nuestros activos más críticos. Dependiendo del número de riesgo que nos ha dado en la evaluación de riesgos, tendrán mayor o menor prioridad para implementar una serie de planes.

Además se citarán algunas iniciativas que se pueden tener en cuenta para mejorar la seguridad de los activos de manera generalizada. Estos planes dependen no solo de la evaluación de riesgo ya que es importante tener en cuenta los recursos de la empresa para llevar a cabo estos proyectos.

Los siguiente proyectos son los que hemos planeado para mitigar los posibles riesgos que nos pueden deparar en corto o largo plazo.

Hemos llegado a la conclusión que **la página web y tienda online** de la empresa deberán ser alojados dentro de la misma empresa para garantizar el acceso y la disponibilidad para los clientes y empleados de nuestra organización. Esta inclusión deberá establecerse en un plazo mínimo de 6 meses y máximo de 12.

El servidor de correo electrónico debe estar siempre disponible ya que se encargará de conectar a los clientes que contacten a través de la web con nuestros empleados. Para que el servidor siempre esté disponible deberá tener un sistema de alimentación ininterrumpido para que no caiga si se corta la electricidad en la empresa.

Se propone hacer este añadido en un plazo también mínimo de 6 meses y máximo de 12 meses.

El servidor de archivos y aplicaciones es el que contiene la información importante sobre nuestros clientes, los proyectos, los proveedores y las empresas que trabajan con nosotros. Las copias de seguridad deben de comprobarse cuando son ejecutadas.

Además, debemos **establecer un sistema de alimentación ininterrumpido** al igual que el servidor de correo para asegurar su disponibilidad. Este plan se debe hacer en un rango de 1 mes a 3 meses ya que no podemos permitirnos perder esta información y debe asegurarse lo antes posible.

Los departamentos mencionados anteriormente son los pilares del plan de negocio de la empresa y por lo tanto debemos **asegurar la disponibilidad de sus dispositivos informáticos todo el tiempo y el acceso a los mismos**, para ello tenemos un firewall y un antivirus que nos asegura la red y los dispositivos pero deberá llevarse a cabo un plan de concienciación para los empleados.

Este *plan de concienciación* debe llevarse a cabo una vez cada 6 meses para cubrir la plantilla de estos departamentos incluyendo a los nuevos integrantes y veteranos.

Se debe llevar a cabo un **documento con las políticas de seguridad** que se deben cumplir en la empresa para los empleados de la misma. Estas políticas deben tener un control para verificar que se cumplen. Este documento debe de llevarse a cabo en un mínimo de un mes y un máximo de tres.

La seguridad de las sedes está a cargo de una empresa subcontratada que pone a nuestra disposición personal de seguridad para proteger el acceso a las mismas de personas ajenas a la empresa y un sistema de vigilancia de cámaras de seguridad. Asignar un responsable que haga de nexo entre nuestra empresa y la subcontrata de seguridad. Este responsable debe implantarse como mínimo en un mes y máximo tres meses.

Los **equipos informáticos** de los jefes de departamento y del consejo de administración son activos igual de importantes ya que siempre deben ser accesibles y seguros. Para ello se debe revisar el antivirus gestionado por la empresa subcontratada e informar a la dirección de la existencia de este contrato.

En caso de que no se apruebe, se deberá analizar qué antivirus del mercado o qué empresa entran dentro de los requisitos que la dirección imponga. Esto debe llevarse a cabo en un mes puesto que la seguridad de los dispositivos es de gran prioridad.

La creación de un **equipo de ciberseguridad** para controlar la seguridad referente a los dispositivos digitales de la empresa e implementar esta serie de iniciativas y proyectos. La creación de este equipo debe ser de un mes a tres meses como máximo.

Crear un **plan de contratación** elaborado en el que se investigue a los candidatos de los puestos de trabajos que se necesiten cubrir. También se deberá eliminar cualquier cuenta de usuario el día anterior al despido de un empleado para evitar el acceso desde el exterior de manera no autorizada. Este plan debe hacerse también a corto plazo con un mínimo de un mes y un máximo de tres.

Crear un **plan de acceso a información basado en roles** para asegurarnos que cierta información sólo puede ser accedida por ciertos empleados tanto de la empresa como de los clientes. De un mes como mínimo a tres meses como máximo.

Se deberá asignar una serie de recursos financieros y de personal de ciberseguridad para llevar a cabo la posible implementación de los planes descritos en este apartado y su supervisión y gestión de la seguridad de estos activos.

5. Clasificación y Priorización de los Proyectos

Teniendo en cuenta las iniciativas y proyectos establecidos, se ha decidido priorizar los proyectos en función a la urgencia de cada uno frente al tiempo que requieren. La clasificación sería la siguiente:

Área	Proyecto	Prioridad
Gestión y desarrollo de la seguridad	Creación de un equipo de ciberseguridad	Alta
	Elaboración de un documento con las políticas de ciberseguridad	Alta

Sistemas físicos	Asegurar servidores de correo junto a los de aplicaciones con sistemas de alimentación ininterrumpidos (SAIs)	Media
	Asignar un responsable que haga de nexo entre la subcontrata de seguridad para las oficinas y nuestra empresa	Baja
Personal y recursos humanos	Establecer charlas de concienciación y difusión de material informativo para formar al personal	Media
	Aplicar nuevas medidas de contratación teniendo en cuenta antecedentes y revisar a los empleados actuales	Media
	Endurecer la normativa con respecto a altas y bajas de la empresa, asegurando que los viejos empleados no tengan acceso a credenciales oficiales	Alta
Infraestructura digital	Asegurar los equipos informáticos de los jefes de departamento	Alta
	Implementación de un servidor privado de la empresa para alojar nuestra página web y aplicaciones	Baja
	Creación de un plan de credenciales y roles de trabajo para asegurar el acceso a datos.	Alta

6. Aprobación del PDS

El Plan Director de Seguridad (PDS) desarrollado ha de ser presentado a la junta directiva de la empresa en cuestión, con el fin de recibir la aprobación del mismo, constituyendo este proceso un hito crítico en la implementación de la estrategia de seguridad diseñada para la compañía. La aprobación del PDS no sólo representa un acto formal, sino un compromiso de la alta dirección con la seguridad de la información y la protección de los activos de la empresa.

El acto de aprobación del PDS supone el respaldo y compromiso de los líderes de la organización con la estrategia de seguridad diseñada y desarrollada, lo que implica por extensión un respaldo financiero a las iniciativas de seguridad propuestas, y la dedicación por promover una cultura de seguridad en la totalidad de la organización.

7. Puesta en Marcha del PDS

Con el objetivo de implementar correctamente la estrategia de seguridad desarrollada para la empresa, se han clasificado y priorizado los proyectos considerados, de modo que facilite el desarrollo de una línea de tiempo a seguir.

Los proyectos prioritarios constituyen las mayores necesidades de la empresa en materia de seguridad, y serán llevados a cabo con preferencia sobre los demás. Entre estos proyectos encontramos:

- Creación de un **equipo de ciberseguridad** entre 1 y 3 meses.
- Elaboración de un **documento con las políticas de ciberseguridad** entre 1 y 3 meses.
- Endurecimiento de la **normativa** referente a las **altas y bajas** de las empresa, lo que conlleva eliminar los usuarios, y por consiguiente el permiso de acceso de los empleados que se vayan a dar de baja. Este proyecto se debe llevar a cabo en un plazo de 1 a 3 meses.
- Creación de **plan de credenciales y roles** que restrinjan el acceso a la mayoría de usuarios, permitiéndolo sólo a los que tengan el nivel adecuado de permisos. Esto debe cumplirse en un plazo de 1 a 3 meses.

- **Asegurar los equipos informáticos** de los **jefes de departamento**, con un plazo establecido de un mes como máximo.

Una vez examinados los proyectos con un nivel de prioridad superior, debemos centrarnos en aquellos con un nivel medio de prioridad, los cuales son:

- Establecer un **sistema de alimentación ininterrumpido** (SAI) para los servidores aplicaciones y de correo en un plazo de 1 a 3 meses.
- Difundir **charlas de concienciación** y formar al personal con **material informativo**, llevándose a cabo con un período de 6 meses.
- **Medidas de contratación** más **estrictas**, teniendo en cuenta los **antecedentes** de los aspirantes, así como realizar una revisión del personal en un plazo de 1 a tres meses.

Finalmente podremos dirigir nuestra atención a los proyectos que, aunque importantes también para la seguridad de la empresa, son los que son etiquetados como los menos prioritarios, los cuales son:

- Asignar un **responsable** que actúe como **nexo** entre la **subcontrata de seguridad** y la propia compañía. Este responsable debe ser designado en un plazo entre 1 y 3 meses.
- Implementación de un **servidor web privado** para alojar la **página web** de la compañía, en un plazo de 6 a 12 meses.

Debe tenerse presente que en la línea de tiempo que la empresa seguirá para implementar los proyectos anteriormente discutidos, es necesario respetar los plazos establecidos, pero teniendo en cuenta en todo momento la prioridad de cada proyecto.

Cada proyecto tiene un coste asociado, de modo que de hallarse en la situación de tener que elegir unos proyectos sobre otros, se impondrá la preferencia sobre los de mayorprioridad, dado que son los más importantes para salvaguardar la seguridad de la compañía.

8. Tareas Asociadas y Responsables

Teniendo en cuenta las medidas establecidas, en este apartado se dividirán las iniciativas en tareas asumibles por una serie de responsables que también se añaden a continuación. Estas tareas surgen directamente de los proyectos e iniciativas de la empresa. Serán las siguientes:

- Reclutamiento de personal especializado en ciberseguridad, montaje y coordinación de su departamento, cuyo responsable será el consejo de administración.
- Elaboración del documento de políticas de seguridad de la empresa por parte del equipo de ciberseguridad.

- Creación y gestión de una matriz de credenciales y roles por parte del equipo de ciberseguridad para garantizar que solo el personal necesario tenga acceso a información sensible.
- Asignación de un responsable de seguridad encargado de mantener contacto con las subcontrata de seguridad física de nuestra empresa por parte del consejo de administración.
- Compra e instalación de múltiples SAIs para asegurar los equipos de nuestra empresa. Responsabilidad del departamento de compras y la instalación por parte del equipo de TIC.
- Elaborar material didáctico en materia de ciberseguridad para distribuir entre los empleados en forma de documentos y charlas informativas. Tarea del equipo de ciberseguridad.
- Redactar nuevas políticas de contratación sobre antecedentes y revisar el historial de los empleados actuales, endurecer las políticas existentes sobre credenciales de seguridad. Es trabajo del departamento de recursos humanos.
- Compra y configuración de una sala de servidores con sus respectivas medidas de seguridad, en los cuales alojaremos nuestra página web en principio, con expectativa de ampliar más servicios alojados. De esto se encargará el departamento de TIC y Compras.
- Bastionado y configuración de los equipos de los jefes de departamento por parte del equipo de ciberseguridad.
- Encargar al equipo de ciberseguridad que gestione la situación del procedimiento existente para el antivirus de la subcontrata, se debe decidir si se va a seguir usando y aprobarlo o descartarlo.
- Elaborar una documentación y mapeo de la red de la empresa para que varios empleados del departamento de TIC la conozcan, los actuales y próximos, no solo el administrador de red actual.

Con estas tareas estarían en principio cubiertos los proyectos propuestos.

9. Conclusiones

El fin último del Plan Director de Seguridad consiste en establecer una base sólida de la estrategia para garantizar la seguridad de la información y de los activos críticos de la organización. Para lograr este objetivo, así como lograr proteger la confidencialidad, integridad y disponibilidad de la información, favoreciendo el éxito en el funcionamiento del negocio, se debe realizar un enfoque en la identificación y mitigación de riesgos, promocionando buenas prácticas de seguridad.

Una vez implementado el Plan de Seguridad, es completamente necesaria la cooperación y compromiso completo de la totalidad de los integrantes de la organización, a fin de garantizar una aplicación exitosa del mismo.

En última instancia se debe tener en cuenta los constantes cambios que suceden constantemente a nuestro alrededor, haciendo evolucionar el ámbito de la seguridad informática en cuestión de pocos años, por lo que como consecuencia el Plan Director de Seguridad jamás debe ser un documento estático, sino un marco dinámico que se adaptará a medida que evolucionen las amenazas y las tecnologías. Su implementación efectiva, teniendo esto en cuenta, permitirá a la compañía mantenerse segura, tanto en el corto como el largo plazo, a mitigar riesgos y a ser una organización resiliente en un entorno en constante cambio.

10. Bibliografía

- https://www.globalsuitesolutions.com/es/como-mejorar-estrategia-de-ciberseguridad-empresa/
- https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf
- https://protecciondatos-lopd.com/empresas/plan-director-de-seguridad/
- https://ayudaleyprotecciondatos.es/2020/10/30/plan-director-de-seguridad/
- https://www.tuv.com/spain/es/sistema-de-gesti%C3%B3n-de-la-continuidad-del-negocio-(bcms).html#:~:text=Un%20sistema%20de%20gesti%C3%B3n%20de%20la%20continuidad%20del%20negocio%2C%20o,los%20desarrolla%20y%20mejora%20continuamente.
- https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio
- https://www.ekon.es/rgpd/

Vídeos de la unidad:

- https://www.youtube.com/watch?v=knxhzpNFWGI
- https://www.youtube.com/watch?v=b9lKThhkGIA
- https://www.youtube.com/watch?v=Ae83EGzerIk
- https://www.youtube.com/watch?v=o33EgLwUl-A