PLAN DIRECTOR DE SEGURIDAD

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

La evolución de las tecnologías de la información y comunicación nos ha permitido automatizar y optimizar muchas de las actividades que se llevan a cabo en nuestra organización. Estas tecnologías han ido ocupando un lugar cada vez más importante, hasta el punto de que hoy en día, sin ellas, muchos de nuestros procesos de negocio no serían posibles.

La información es un activo importante para las empresas, es fundamental para el negocio: facturas, informes, bases de datos de clientes, pedidos, etc. Podemos decir que las empresas basan su actividad en **sistemas de información** con soporte tecnológico (ordenadores, tabletas, página web,...)

Por eso proteger los sistemas de información es proteger el negocio. Para garantizar la seguridad de la información del negocio se necesita llevar a cabo una gestión planificada de actuaciones en materia de Ciberseguridad, tal y como se realiz en cualquier otro proceso productivo de la organización.

1.1. ¿QUÉ OCURRIRÍA SI NUESTRA EMPRESA SE ENCONTRASE EN ALGUNA DE LAS SIGUIENTES SITUACIONES?

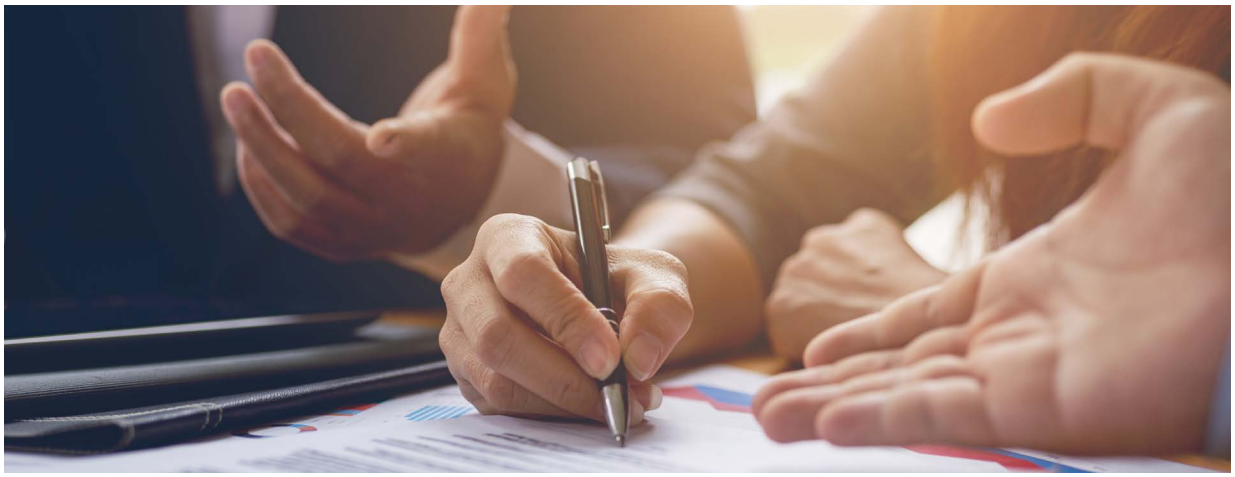
- Sufrimos los efectos de un virus informático y no sabemos cómo reaccionar.
- Se produce una pérdida de datos y no tenemos copias de seguridad **[1]** o no podemos recuperar la información.
- Perdemos o extraviamos un disco duro portátil con información sensible.
- Nuestra página de comercio electrónico es el objetivo de un ataque de denegación de servicio, dejándola inoperativa.
- Se nos estropea algún servidor o elemento de red, que nos impide el uso del correo electrónico, la conexión a Internet o el uso de una aplicación crítica.

Frente a escenarios como los anteriores, surgen muchas dudas:

- ¿Debería externalizar el soporte informático de mi empresa?
- ¿Es seguro gestionar información corporativa en dispositivos móviles? ¿hemos proporcionado y utilizado los recursos necesarios para ello?
- ¿Sabemos si las copias de seguridad funcionan? ¿estamos realizando copias de toda la información crítica para nuestra organización?

Si sufrimos un incidente de seguridad informática, ¿conocemos los riesgos a los que está expuesta nuestra empresa?

Si las herramientas tecnológicas y la información que dan soporte a los servicios y procesos productivos de la organización son de gran valor para nuestra organización, debemos empezar a pensar en poner en práctica un **Plan Director de Seguridad.**



1.2. ¿QUÉ ES UN PLAN DIRECTOR DE SEGURIDAD?

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

Es fundamental para la realización de un buen Plan Director de Seguridad, en adelante PDS, que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboren con ésta.

2. IMPLANTANDO UN PLAN DIRECTOR DE SEGURIDAD

Los proyectos que componen el Plan Director de Seguridad varían en función de diversos factores relacionados como:

- El tamaño de la organización
- El nivel de madurez en tecnología
- El sector al que pertenece la empresa
- El contexto legal que regula las actividades de la misma
- La naturaleza de la información que manejamos
- El alcance del proyecto
- Otros aspectos organizativos

Estos factores determinarán la magnitud y complejidad del Plan Director de Seguridad resultante. No obstante, en general, para la elaboración y puesta en marcha de un Plan Director de Seguridad se siguen las fases o etapas que muestra la ilustración 1:

Siempre debemos tener presente que un Plan Director de Seguridad, se basa en la mejora continua. Por tanto cuando hayamos finalizado debemos comenzar de nuevo el ciclo.

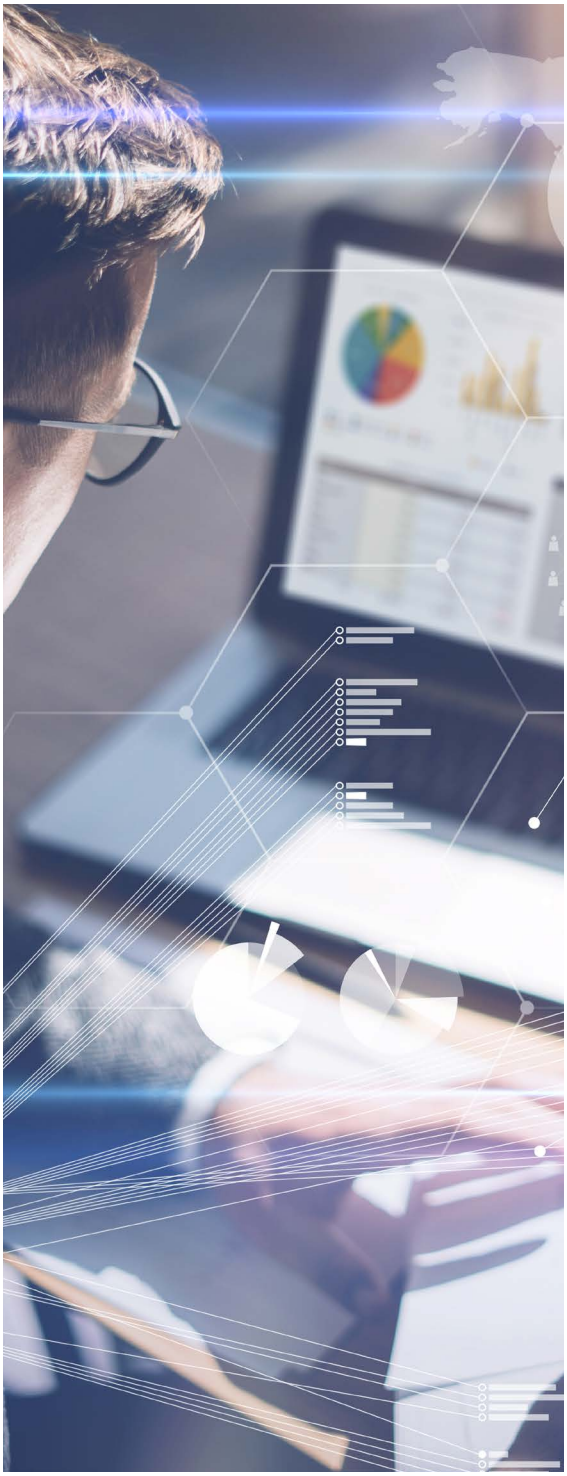
Ilustración 1
Implantando un Plan Director de Seguridad

2.1. CONOCER LA SITUACIÓN ACTUAL DE LA ORGANIZACIÓN (FASE 1)

La primera fase consiste en conocer la situación actual de nuestra empresa en materia de ciberseguridad. Para ello debemos llevar a cabo distintos análisis considerando aspectos técnicos, organizativos, regulatorios y normativos, entre otros.

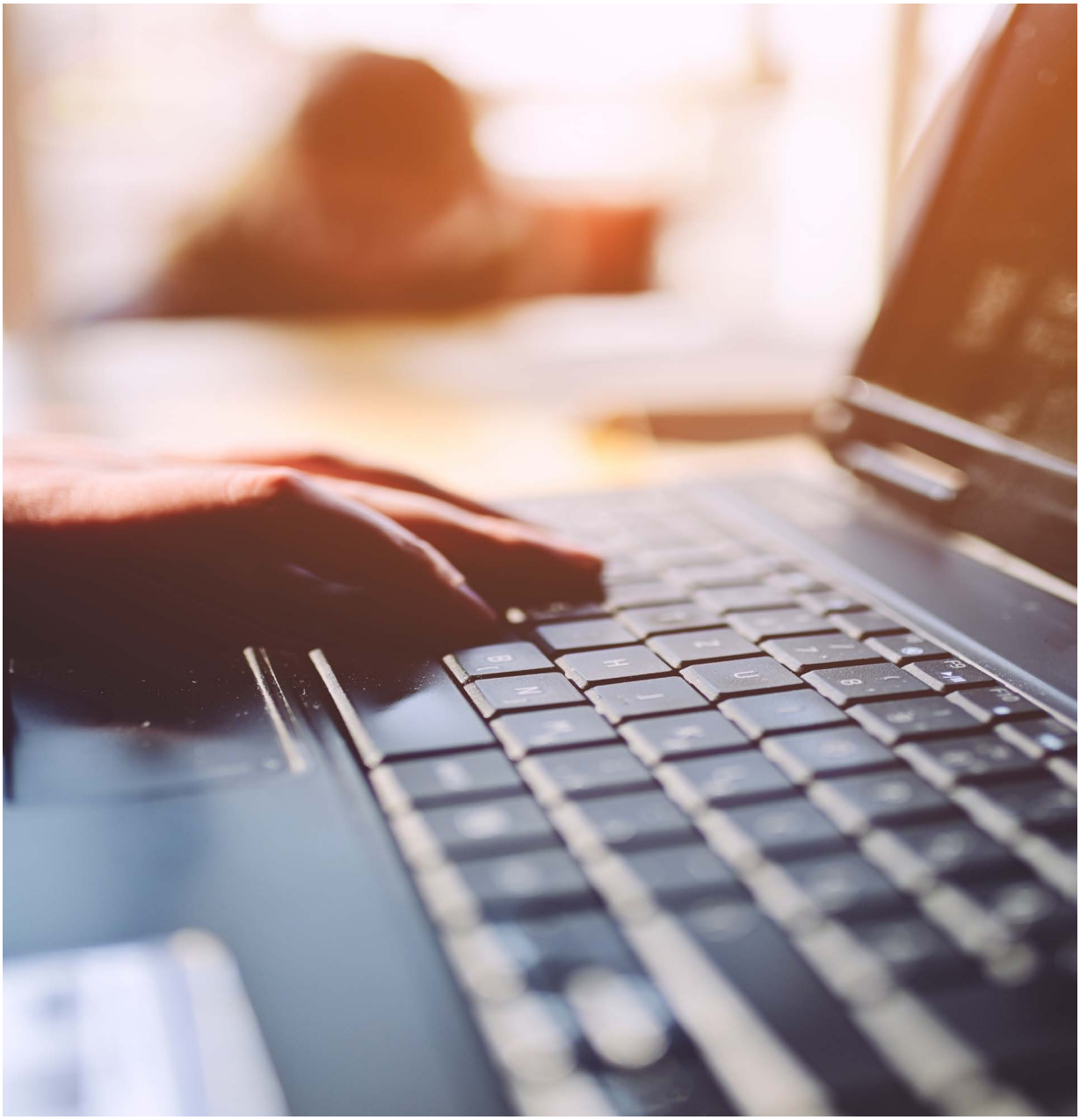
Esta es la fase más importante y compleja de la elaboración del Plan Director de Seguridad, debido a la participación de diferentes personas y a la importancia que tiene que la información de la organización necesaria para conocer y evaluar su situación actual, sea fiable, completa y actualizada.

En esta fase es fundamental contar con el **apoyo de la Dirección**. Éste es un aspecto esencial para garantizar el éxito del Plan Director de Seguridad, dado que este respaldo garantizará no sólo que disponemos de suficientes recursos, sino que el enfoque del proyecto está alineado con la filosofía y estrategia de la empresa.



2.1.1. ACTIVIDADES PREVIAS

Antes de comenzar con el primer paso del análisis, debemos realizar varias actividades previas:



2.1.1.1. Acotar y establecer el alcance

Es esencial definir claramente el alcance sobre el que vamos a desarrollar el PDS. Este alcance determinará la magnitud de los trabajos y también cuál será el foco principal de la mejora tras la aplicación del PDS.

> Como posibles alcances podemos escoger: un único departamento (habitualmente el de TIC), un conjunto de procesos críticos, o unos sistemas específicos.

Lo recomendable es determinar aquellos **activos y procesos de negocio críticos**, aquellos sin los que la empresa no puede subsistir, y utilizar éstos como alcance del PDS. De esta manera, la ejecución del PDS tendrá un impacto más positivo sobre la seguridad de la información de la organización.

> Si el proceso más crítico de nuestra empresa está relacionado con el proceso de facturación, podemos limitar el alcance a éste: sistemas y equipos implicados, personal, aplicaciones necesarias, riesgos específicos, etc. Aunque las mejoras serán específicas dentro de este proceso, nos permitirá profundizar en el resultado y partir de un punto para extenderlo a otros departamentos o procesos.

2.1.1.2. Responsables de la gestión de los activos

Los activos de la organización son todos aquellos que tienen valor para ella. Así los **activos de información** son todos los procesos, personas, equipos, instalaciones, software o ficheros de todo tipo que la contienen, procesan o manejan de alguna forma.

Por ello es importante definir las **responsabilidades sobre los activos** de la organización: equipos informáticos, dispositivos móviles, aplicaciones, instalaciones (CPD), servicios e información. Esto nos facilitará hacer un seguimiento de la ejecución de las iniciativas implantadas, así como del análisis y recogida de la información.

Dichas responsabilidades deben estar asociadas a perfiles específicos, ya sea una persona o un comité formado por varias personas. En el caso de empresas de pequeño tamaño, varios de estos roles pueden ser asumidos por la misma persona (el propietario del activo en cuestión).

Al menos, se deben definir los siguientes perfiles:

- **Responsable de Seguridad,** con la finalidad de hacer un seguimiento y coordinar todas las iniciativas puestas en marcha por la organización en materia de Seguridad de la Información.
- **Responsable de Información,** especialmente cuando tratamos con información específica que es gestionada a través de diferentes entornos.
- **Responsables de ámbito,** en el caso de que pongamos en marcha iniciativas en el ámbito lógico, físico, legal y organizativo.

> Los controles de seguridad física pueden ser responsabilidad del responsable del área de Mantenimiento o Servicios Generales, mientras que los aspectos legales serán responsabilidad del responsable del área Jurídica. Todos estos deberán ser coordinados por el Responsable de Seguridad, garantizando su correcta ejecución.

2.1.1.3. Valoración inicial

Un buen comienzo implica **realizar una valoración preliminar** de la situación actual de la organización para determinar los controles y requisitos que son de aplicación. En la jerga de Gestión de la Seguridad se llaman **controles** a las medidas de todo tipo (técnico, legal u organizativo) que se implementan para contrarrestar los riesgos de seguridad.

Por norma general, la **evaluación de los aspectos normativos y regulatorios** la realizaremos tomando como referencia el estándar internacional ISO/IEC 27002:2017 **[2]**, diseñada para ser utilizada a la hora de designar controles para la selección e implantación de un Sistema de Seguridad de la Información, así como unas directrices de Gestión de la Seguridad de la Información.

> Los controles relacionados con la gestión de copias de seguridad, requerimientos legales como cumplir con el RGPD **[3]**, instalación de cortafuegos o la definición de un plan de continuidad del negocio.

El conocimiento de esta norma es imprescindible para el desarrollo adecuado de un Plan Director de Seguridad. No es necesaria la implementación de todos los controles que se indican en la norma 27002:2017, sino sólo aquellos que sean de aplicación a nuestra empresa.

> Si nuestra empresa no desarrolla aplicaciones, no tendremos que valorar aquellos controles de esta norma que hagan referencia al desarrollo seguro de aplicaciones.
>
> Si nuestra empresa no proporciona un servicio de comercio electrónico, no será necesario que apliquemos los controles relacionados con la transacción de datos personales en la compra-venta online.
>
> Por el contrario, sí será necesario aplicar medidas o controles relacionados con las copias de seguridad o el proceso de altas y bajas de personal, ya que éstos serán de aplicación

Después de analizar los controles según la norma, elaboraremos un documento con los controles o medidas de seguridad que aplican en la organización y su grado de madurez, es decir, si están implantados y en qué estado están. A este documento lo llamaremos «Documento de Selección de Controles». En la norma se refieren al mismo como «Declaración de Aplicabilidad» o «SOA» por sus siglas del inglés *Statement of Aplicability*».

Modelo de madurez

A modo orientativo, podemos partir de una escala de madurez de cinco niveles como la siguiente, basada en el Modelo de Madurez de Capacidades o CMM por sus siglas en inglés:

- **Inexistente.** No se lleva a cabo el control de seguridad en los sistemas de información.

> Aplicándolo a la realización de copias de seguridad en la organización, en este nivel de madurez no se realizarían.

- **Inicial.** Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.

> Aplicándolo al ejemplo de las copias de seguridad, en este nivel de madurez se realizan sin procedimiento y sin planificación.

- **Repetible.** La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.

> En nuestro caso de copias de seguridad, las copias sí se realizan con procedimientos y planificación ad-hoc.

- **Definido.** El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
- **Administrado.** El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
- **Optimizado.** El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.

2.1.1.4. Análisis de cumplimiento

1 Para llevar a cabo el análisis de cumplimiento y situación debemos:

Realizar **reuniones con el personal** de los distintos departamentos de la organización para evaluar el cumplimiento de los controles de seguridad implantados.

Aunque la mayor parte de los controles corresponden al departamento TIC, también es necesario analizar procesos de otras áreas. Habitualmente se incluyen los departamentos de Personal, Jurídico, Administración, Servicios Generales y, en caso de existir, el departamento de Calidad.

Para poder desempeñar adecuadamente las tareas de recopilación de información, es vital que la Dirección traslade a cada una de las áreas y sus responsables la importancia del proyecto, los beneficios derivados de su implantación así como la implicación que se espera de ellos en todas las fases del proyecto.

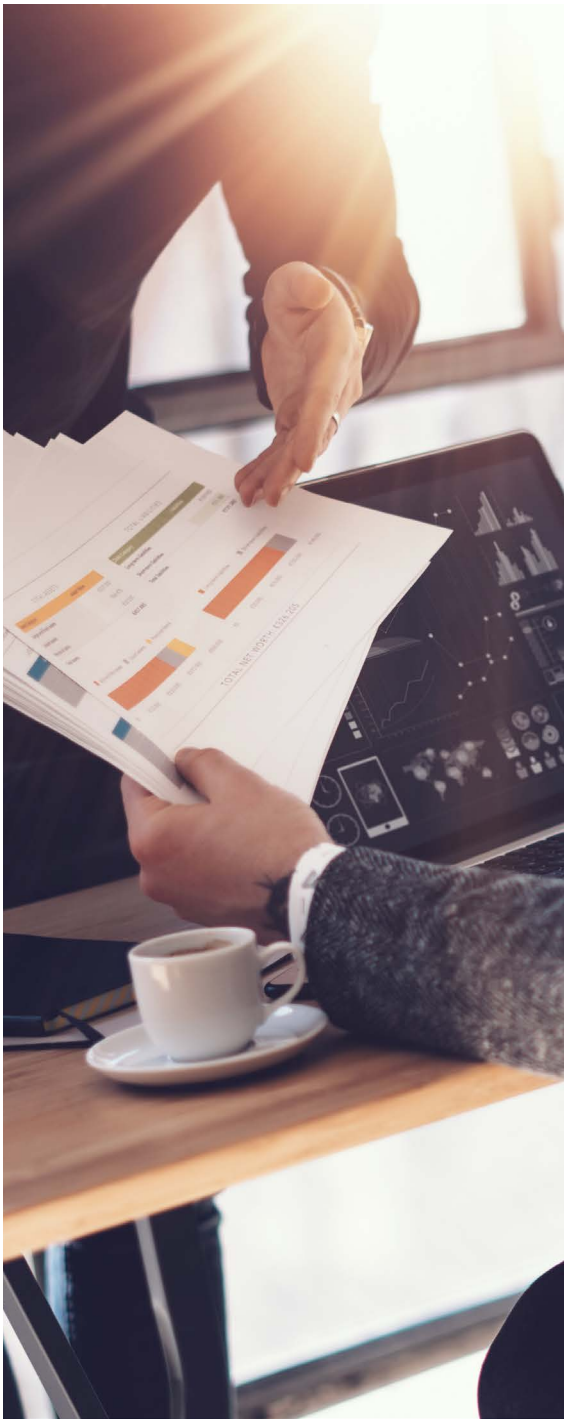
2 Los estándares y normas internacionales en materia de seguridad de la información incluyen requisitos para implantar medidas de control de acceso físico y seguridad medioambiental. Por lo tanto, también será necesario llevar a cabo una **inspección in-situ de las instalaciones.**

3 **Registrar todos los problemas y evidencias** que vayamos detectando, en relación a los requisitos de seguridad de aplicación y que están prefijados, en documentos que luego podamos contrastar y consultar. Por norma general, es muy útil emplear formularios y listas de verificación (checklists) que incluyen los aspectos a revisar y comprobar.

4 Una vez dispongamos de toda la información, debemos **analizar los resultados** y situar el cumplimiento de cada control en una escala, por ejemplo entre el 0 al 5, según el modelo de madurez, donde 0 es la ausencia total del control, y el 5 la aplicación optimizada del control.

> Por ejemplo, trasladando la escala a las copias de seguridad: el nivel 0 sería la ausencia de copias de seguridad, y el nivel 5 la realización de copias, existencia de procedimientos, pruebas de recuperaciones periódicas, análisis periódico de incidencias, etc.

Esta escala nos permitirá conocer la evolución en el tiempo del grado de seguridad de la organización.



2.1.1.5. Establecer los objetivos

Por último, debemos **establecer cuáles son nuestros objetivos** a cumplir en materia de ciberseguridad de la empresa, lo que nos permitirá determinar los ámbitos a mejorar e identificar los aspectos en los que debemos focalizar nuestros esfuerzos.

A continuación, podemos ver un ejemplo de los resultados de la evaluación de los aspectos normativos y regulatorios en una organización tomando como referencia la norma ISO/IEC 27002:2017.

La línea roja representa el grado de cumplimiento actual, la línea amarilla un posible objetivo de cumplimiento a medio / largo plazo y, por último, la línea verde representa el nivel de cumplimiento óptimo. Los números que se muestran en la gráfica hacen referencia a los diferentes dominios contemplados en el estándar.

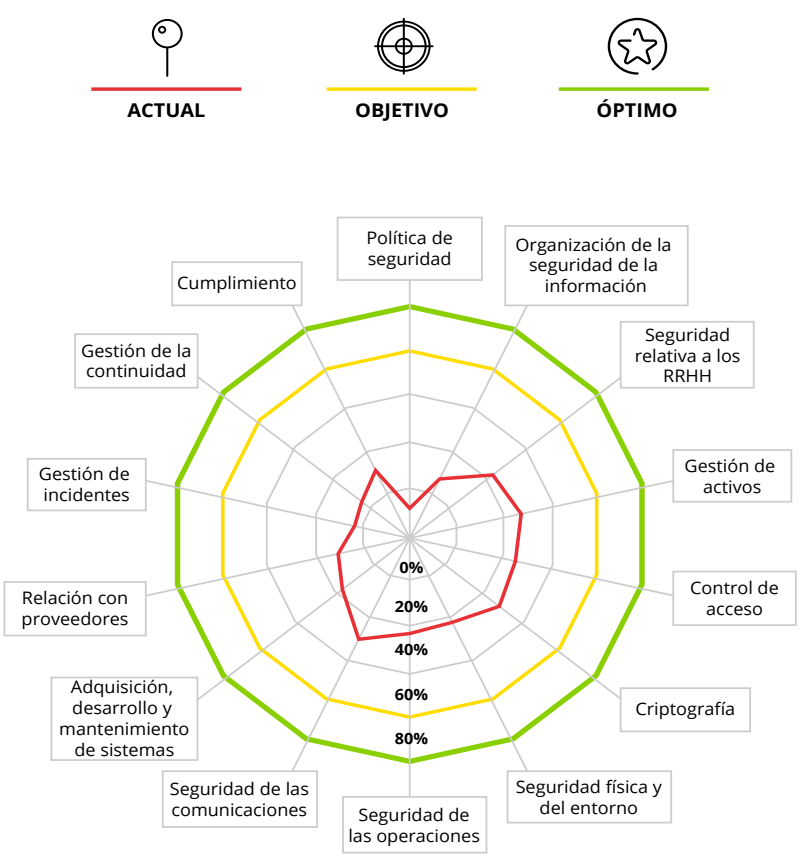


Ilustración 2
Gráfico ejemplo del resultado de la evaluación

Además de la evaluación de la Seguridad de la Información respecto a esta guía de buenas prácticas, para la valoración de los aspectos normativos y legales puede ser necesario tomar como referencia otros estándares o normativas específicos, u otras leyes como el Reglamento General de Protección de Datos (RGPD), detallada en los dosieres de **Protección de Información y Cumplimiento Legal.**

Otros estándares relevantes son el de PCI-DSS si gestionamos datos de tarjetas de crédito; COBIT si queremos optar por guías de buenas prácticas alternativas a la norma ISO 27002 o el Esquema Nacional de Seguridad si trabajamos habitualmente con información de la Administración Pública o les proporcionamos servicios.

2.1.2. ANÁLISIS TÉCNICO DE SEGURIDAD

Por otra parte, el análisis técnico de la seguridad queda cubierto mediante la valoración del grado de implantación y madurez de los controles más relacionados con los sistemas de información empleados por la organización para almacenar y gestionar su información.

Además de temas de gestión y de evaluación de controles en base a entrevistas y percepciones, la realidad del estado de seguridad de una organización se evidencia mediante la comprobación y valoración de aspecto tales como:

- Si disponemos de antivirus y cortafuegos.
- Si nuestra página web es segura.
- Si la red está correctamente segmentada, que impida por ejemplo que desdeInternet sean visibles los equipos de los usuarios o los servidores internos.
- Si existen controles de acceso físicos a las áreas con información sensible:salas de servidores, despachos, área de Recursos Humanos, etc.

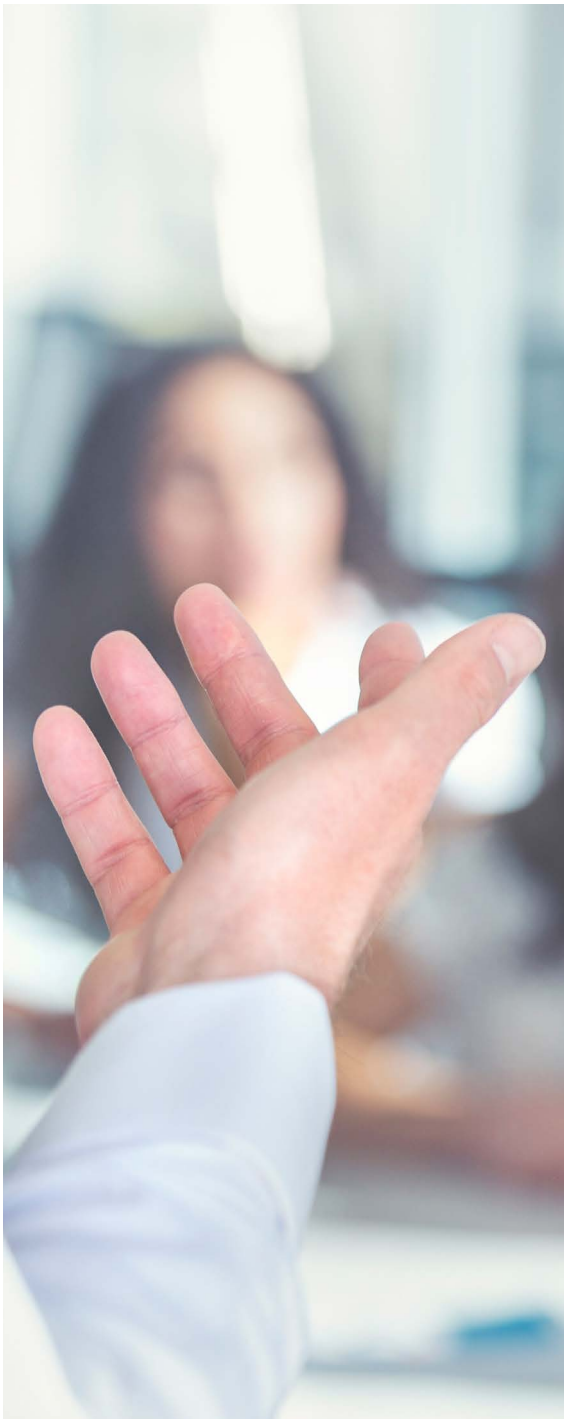
Estas pruebas nos permiten identificar deficiencias en la seguridad técnica de la organización, y a través de ellas, comprobamos la eficacia de los controles de seguridad lógica existentes en la organización: cortafuegos, antivirus, sistemas de detección de intrusos, niveles de parcheado, política de contraseñas, etc.

El alcance y modalidad de esta auditoría puede variar en función de la estrategia de negocio, el ámbito de nuestra empresa y nuestros antecedentes. Así, una empresa de comercio electrónico puede estar interesada en la seguridad de su página web, mientras que una empresa con otros riesgos diferentes en cuanto a fuga de información puede estar más interesada en mejorar el proceso de alta y baja de empleados, políticas de buenas prácticas del uso del correo corporativo, **cultura en seguridad** o los controles de acceso, entre otros.

Debido a que se trata de un trabajo especializado, es habitual que la organización opte por **externalizar el análisis técnico de la seguridad.** En estos casos debemos prestar especial atención a la coordinación del equipo externo con el personal propio de nuestra organización, para establecer el tipo de pruebas a realizar y el método de trabajo que se utilizará. Por norma general, debemos requerir que no se lleven a cabo pruebas «agresivas», en cuanto a carga de trabajo de sistemas o redes, que pudieran afectar a la disponibilidad de los servicios TIC.

Por contra, si optamos por llevar a cabo estas pruebas de forma interna, es fundamental acotar el periodo de realización y que el personal TIC prepare, previamente, procedimientos de recuperación sobre los entornos que serán evaluados, con el fin de minimizar el impacto en el negocio.

Es recomendable que se lleven a cabo auditorías técnicas tanto desde el exterior de la organización como desde el interior. De este modo podremos ponernos en el papel tanto de un atacante interno, por ejemplo un empleado malintencionado, como en el de un atacante externo, por ejemplo un ciberdelincuente.



2.1.3. ANÁLISIS DE RIESGOS

Paralelamente al desarrollo de los trabajos de auditoría, es necesario que realicemos un **análisis de riesgos [4]** a los que está expuesta nuestra organización.

Para llevarlo a cabo, podemos identificar las siguientes etapas:

Como resultado de este análisis de riesgos, obtendremos el conjunto de amenazas a las que estamos expuestos.

Ilustración 3
Etapas del Análisis de Riesgos

Existe una gran variedad de metodologías para el análisis de riesgos, habitualmente, éstas presentan aspectos comunes como, por ejemplo, la necesidad de identificar los activos de la organización y su valor.

En el siguiente diagrama, podemos identificar gran parte de los elementos que intervienen en un análisis de riesgos.

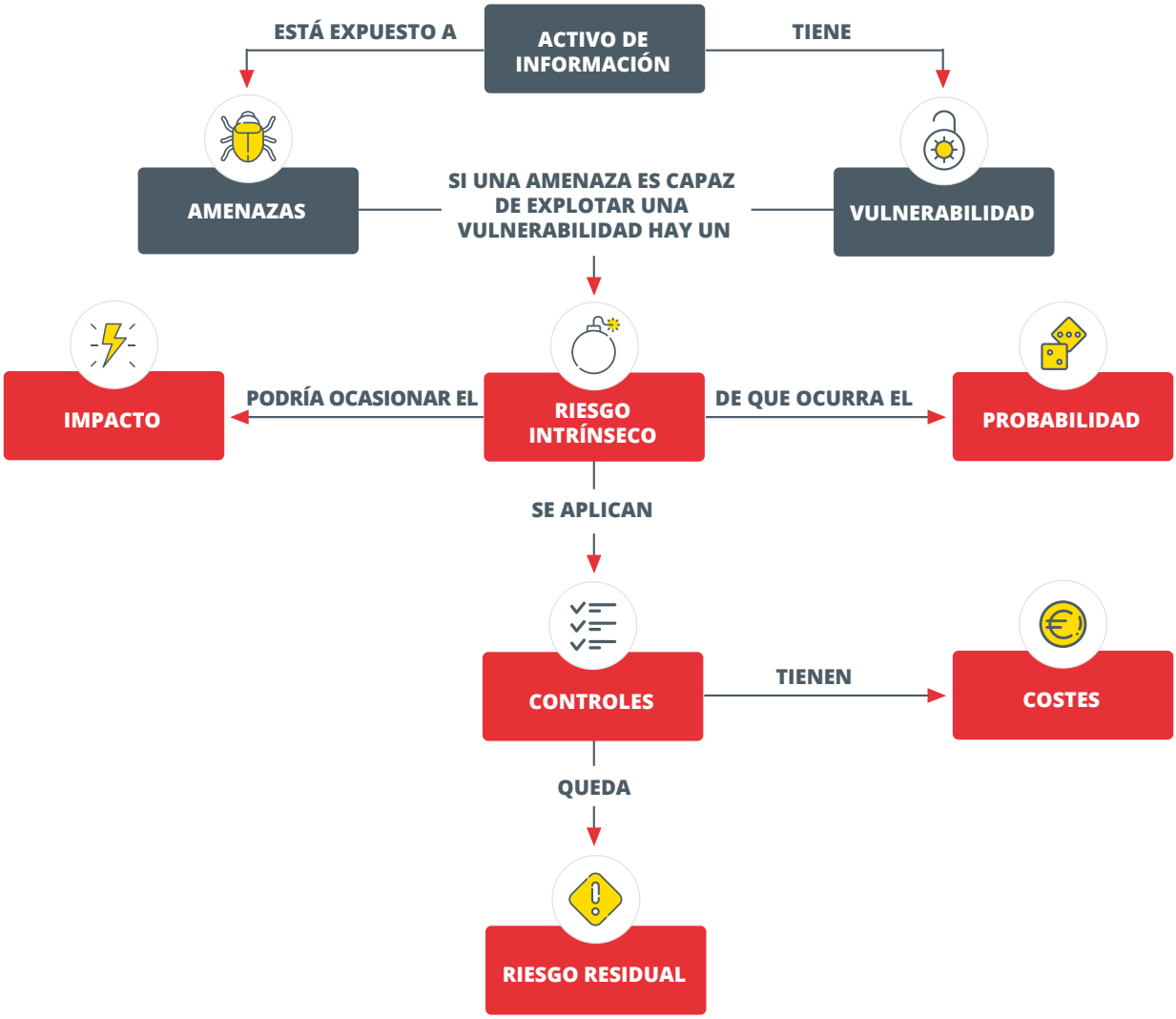


Ilustración 4
Elementos de la Gestión de la Seguridad de la Información

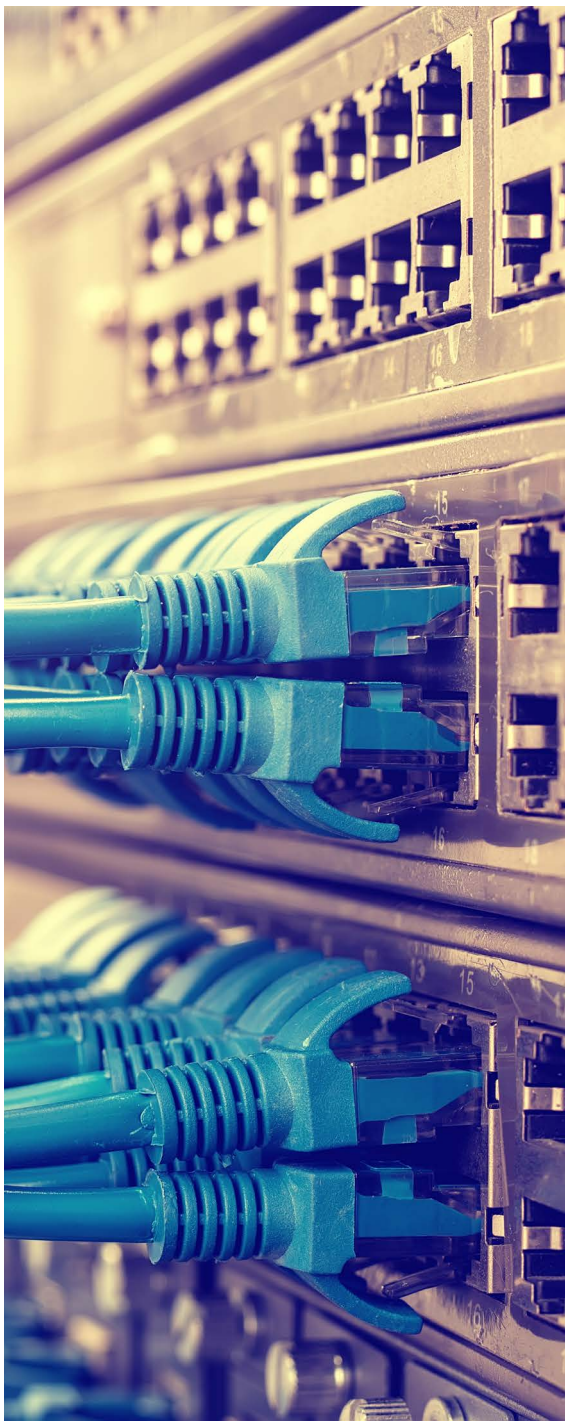
El proceso para realizar un análisis de riesgos consta de los siguientes pasos:

1 Identificar los **activos de información** de nuestra organización, cada uno de los cuales estará expuesto a unas **amenazas** determinadas y tendrá unas **vulnerabilidades** asociadas.

> Un servidor web puede estar expuesto a una denegación de servicio y tener como vulnerabilidad poca tolerancia a una carga de tráfico excesiva.

2 Del paso anterior, que nos describe el estado del activo, obtenemos el **riesgo intrínseco**. Es decir, el riesgo al que está expuesto el activo «por defecto» antes de la aplicación de los controles específicos.

3 En el paso siguiente, determinamos la **probabilidad** de materialización de un riesgo intrínseco, que dará como resultado un impacto, es decir, las consecuencias que tiene para nuestra organización la materialización de la amenaza.



4 A continuación, debemos identificar aquellos **riesgos** que, por su probabilidad, impacto o ambos, **no** son **aceptables** para nuestra organización. Esta decisión debemos tomarla de acuerdo a nuestra estrategia corporativa y en función de los riesgos que estemos dispuestos a asumir.

Para aquellos riesgos que no sean aceptables, debemos proponer diferentes iniciativas para la implantación de controles o salvaguardas, que tendrán un coste asociado.

En algunos casos, este coste es determinante para escoger controles menos eficaces pero con un menor coste o para asumir el riesgo debido al alto coste del control mitigante.

5 Como resultado de la aplicación de los controles, obtendremos el **riesgo residual** del activo, que nos indicará el grado de exposición del activo a las amenazas después de haber implantado los controles seleccionados así como las consecuencias de la materialización de la amenaza.

Tendremos en cuenta que los elementos y valores anteriores son dinámicos y podrán cambiar a medida que nuestra infraestructura evolucione, se añadan nuevos activos, ofrezcamos nuevos servicios, surjan nuevas amenazas o apliquemos unos controles determinados.

> La sustitución de un sistema de copias tradicional por un sistema de replicación de datos en diferido puede eliminar riesgos de disponibilidad pero incrementar los riesgos de disponibilidad e integridad de los datos, al propagarse éstos en la réplica de manera automática.

También podemos crear nuestra propia metodología específica a partir de las existentes. En este sentido, puede resultar interesante adaptar diversas metodologías para obtener una que se adapte a la naturaleza de nuestra organización.

2.1.3.1. Nivel de riesgo aceptable

Tras la identificación de los riesgos debemos establecer y documentar el **nivel de riesgo aceptable**: el valor umbral que determina los riesgos que deben ser tratados y los riesgos que son asumibles. ¿Cómo podemos tratar un riesgo? A través de cuatro posibles estrategias:

- **Transferir** el riesgo a un tercero.

> Por ejemplo, contratando un seguro.

- **Eliminar** el riesgo.

> Eliminando un proceso que ya no es necesario.

- **Asumir** el riesgo, siempre justificadamente.

> El coste de instalar un grupo electrógeno o disponer de un centro de respaldo en caso de interrupción del suministro eléctrico puede ser demasiado alto y por tanto, puede ser necesario asumir el riesgo durante varias horas, a pesar de su impacto.

- **Implantar** medidas para mitigarlo.

> Instalando un sistema de alimentación ininterrumpida o SAI para hacer frente a los cortes de electricidad más breves, o tener algún tipo de acuerdo recíproco con otra compañía para en caso de que se produzca un incidente grave poder usar sus servidores o instalaciones.

En resumen, el análisis de riesgos desarrollado en el contexto del Plan Director de Seguridad está enfocado principalmente a identificar aquellos riesgos que exceden unos límites aceptables para la organización.

Todos los trabajos desarrollados hasta el momento están fuertemente relacionados y en todos los casos requieren de la intervención de múltiples personas que conozcan la organización. En este sentido, nuevamente destacamos la importancia de contar con el apoyo de la Dirección para garantizar el éxito del proyecto.

2.2. CONOCER LA SITUACIÓN ACTUAL DE LA ORGANIZACIÓN (FASE 2)

La segunda fase de la realización de un Plan Director de Seguridad consiste en conocer la estrategia corporativa de nuestra organización.

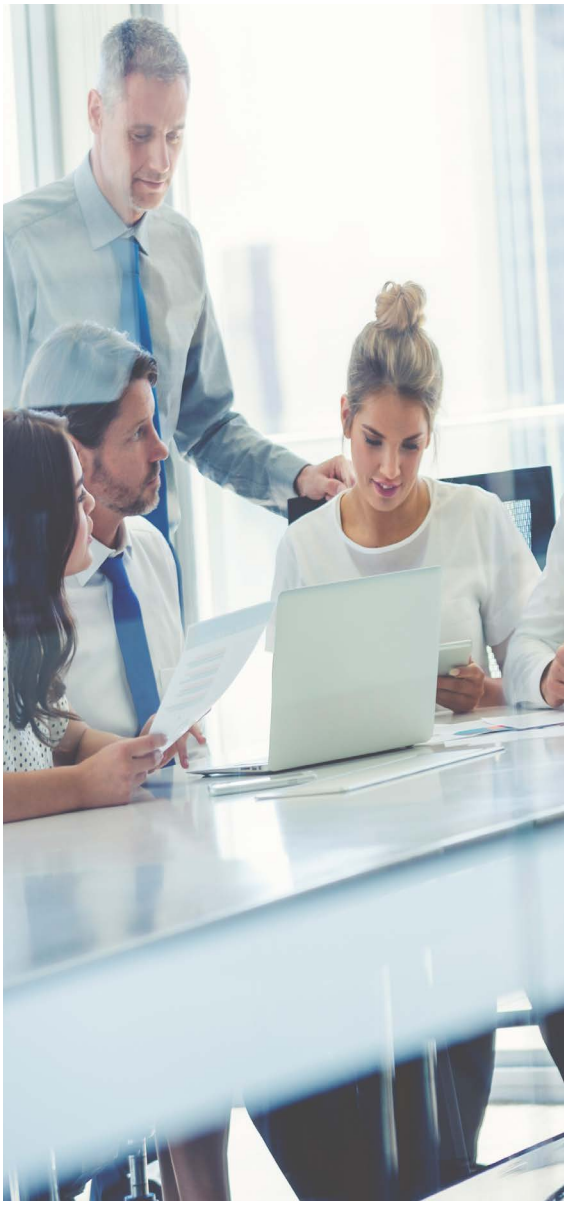
Esto implica considerar los proyectos en curso y futuros, previsiones de crecimiento, cambios en la organización debido a reorganizaciones, etc. También es importante tener en cuenta si nuestra organización opta por una estrategia de centralización de servicios, por la externalización de los servicios TIC, si forma parte de un grupo empresarial mayor o si va a iniciar la actividad en algún sector distinto del actual que pueda generar requisitos legales adicionales.

Todos estos factores pueden afectar a la orientación de las medidas y al peso de cada una de ellas.

Aunque en términos de esfuerzo y coste temporal, esta fase tiene menos peso que las restantes, su importancia es fundamental ya que nos permitirá implantar medidas de seguridad acordes a la naturaleza de nuestra organización.

Esta fase permite alinear la estrategia de seguridad no sólo con la estrategia TIC, sino también con la estrategia general de negocio de la organización.

Para el correcto desarrollo de esta fase, se recomienda analizar la estrategia de la organización con los responsables de los departamentos implicados y por supuesto, con la Dirección. Se obtienen así dos objetivos. En primer lugar, se les hace partícipes en el proyecto y, en segundo lugar, conseguiremos tener una visión objetiva y global de la estrategia de negocio.



2.3. DEFINICIÓN DE PROYECTOS E INICIATIVAS (FASE 3)

A partir de la información recabada hasta este momento, debemos definir las acciones, iniciativas y proyectos necesarios para alcanzar el nivel de seguridad que nuestra organización requiere.

Dado que el análisis realizado incluye diferentes ámbitos como Recursos Humanos, Dirección, Mantenimiento, Jurídico, etc., las iniciativas para subsanar las deficiencias detectadas también serán de distinta índole:

1 En primer lugar, definiremos las iniciativas dirigidas a mejorar los métodos de trabajo actuales, para que contemplen los controles establecidos por el marco normativo y regulatorio.

2 En segundo lugar, pondremos en marcha un conjunto de acciones relacionadas con los controles técnicos y físicos cuya ausencia o insuficiencia hemos detectado.

3 En tercer lugar, definiremos la estrategia a seguir así como los proyectos más adecuados para gestionar los riesgos por encima de nuestro riesgo aceptable.

En la medida de lo posible, debemos estimar el coste de las iniciativas propuestas en términos temporales y económicos, contemplando los recursos materiales como humanos necesarios, tanto a nivel interno como externo.

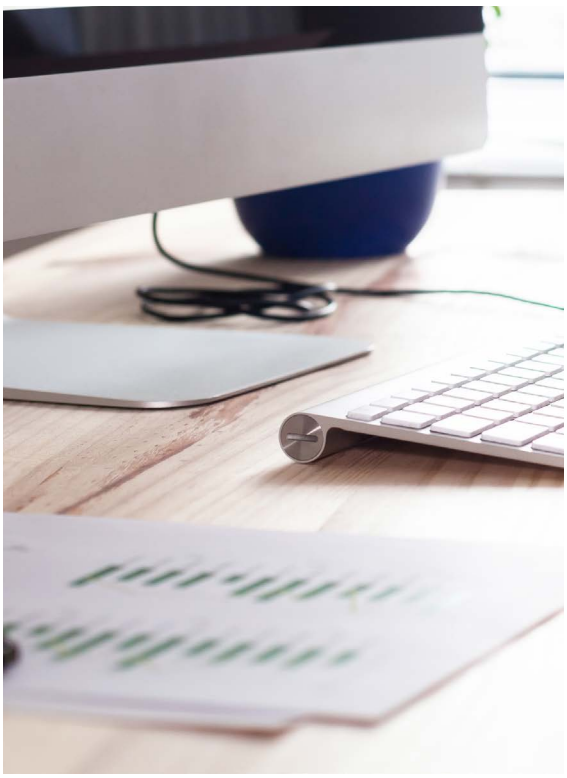
> A modo orientativo, a continuación se incluyen una serie de iniciativas / proyectos «tipo» que frecuentemente forman parte del Plan Director de Seguridad.

ID	PROYECTO	DESCRIPCIÓN
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. › Aspectos de protección de datos.
02	Desplegar un plan de concienciación en materia de seguridad de la información.	Llevar a cabo sesiones de formación y concienciación que cubran tanto el personal de los departamentos operativos como la Dirección.
03	Mejora en la gestión de incidentes y atención al usuario	Definir, documentar e implantar un proceso para la gestión de los incidentes de seguridad.
04	Adecuación al RGPD	Llevar a cabo un proyecto para adaptar la organización al RGPD.
05	Mejorar la coordinación entre el departamento de RRHH y el departamento TIC	Mejorar la capacidad de respuesta de la organización para hacer frente a una contingencia TIC.
06	Desarrollar un Plan de continuidad TIC	Llevar a cabo acciones técnicas para la segmentación de la red corporativa y posteriormente implantar sistemas de detección de intrusos (IDS).
07	Mejoras en la seguridad de la red corporativa	Mejorar la capacidad de respuesta de la organización para hacer frente a una contingencia TIC.
08	Política de copias de seguridad	Realizar un análisis de la información corporativa de la que se realiza copia e implantar una política de copias adecuada, que implique la realización de restauraciones periódicas.
09	Clasificación de la información	Definir un sistema de clasificación de la información que contemple al menos tres niveles de seguridad (público, privado y confidencial). Este sistema debe contemplar aspectos como el etiquetado, acceso, destrucción de la información, uso de cifrado, etc.
10	Regulación de los servicios TIC prestado por terceros	Revisar y homogeneizar los contratos establecidos con los proveedores TIC externos a fin de garantizar que estos son adecuados a las necesidades de la organización. Para aquellos que sean críticos, establecer acuerdos de nivel de servicio.

Tabla 1
Iniciativas/Proyectos en un PDS

Nuevamente, debemos señalar la importancia de considerar la estrategia de la organización a la hora de definir las iniciativas a implantar.

> Si está previsto que la organización pase a formar parte de un grupo empresarial que presta servicios TIC centralizados a todas las sociedades del mismo, se procurará evitar inversiones en activos TIC locales ya que estos podrían no ser amortizados.



2.4. CLASIFICAR Y PRIORIZAR LOS PROYECTOS A REALIZAR (FASE 4)

Una vez identificadas las acciones, iniciativas y proyectos, debemos clasificarlas y priorizarlas. El detalle y granularidad de las acciones a llevar a cabo puede ser muy variado. Ante esta situación, es recomendable agrupar las iniciativas o dividir las propuestas para homogeneizar el conjunto de proyectos que hemos definido.

A la hora de clasificar las iniciativas podemos considerar como criterio el origen de las mismas (es decir, derivadas de la evaluación del cumplimiento normativo y regulatorio, análisis técnico o análisis de riesgos); el tipo de acción (técnica, organizativa, regulatoria, etc.).

Sin embargo, con independencia de que consideremos estos criterios, es conveniente organizar los proyectos atendiendo al esfuerzo que requieren y a su coste temporal. De este modo se establecen proyectos a corto, medio y largo plazo.

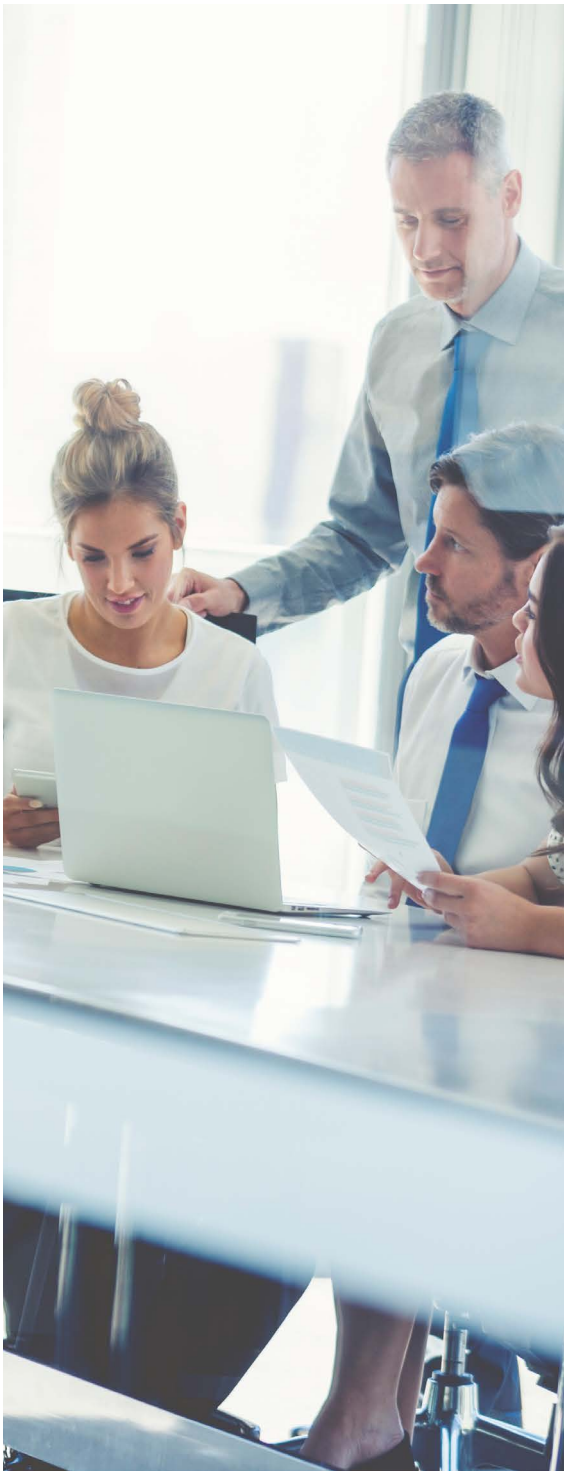
Adicionalmente, es muy aconsejable que creemos un grupo que reúna aquellos proyectos cuya consecución requiere poco esfuerzo pero su resultado produce mejoras sustanciales en la seguridad. Tradicionalmente este tipo de iniciativas reciben el nombre de «*quick wins*».

2.5. APROBAR EL PLAN DIRECTOR DE SEGURIDAD (FASE 5)

En este punto, ya dispondremos de una versión preliminar del Plan Director de Seguridad. Este plan debe **revisarlo y aprobarlo la Dirección.**

Es posible que al revisar el Plan Director de Seguridad haya que modificar su alcance, duración o la prioridad de algunos proyectos. Si fuera preciso, el proceso de revisión se repetirá cíclicamente hasta disponer de una versión final aprobada formalmente por la Dirección.

Una vez disponible la **versión final aprobada por la Dirección**, es conveniente que ésta traslade a todos los empleados de la organización (mediante reunión del director con todos los empleados o mediante correo electrónico) el respaldo al Plan Director de Seguridad, y la importancia del deber de colaborar de toda la organización en la implantación del mismo.

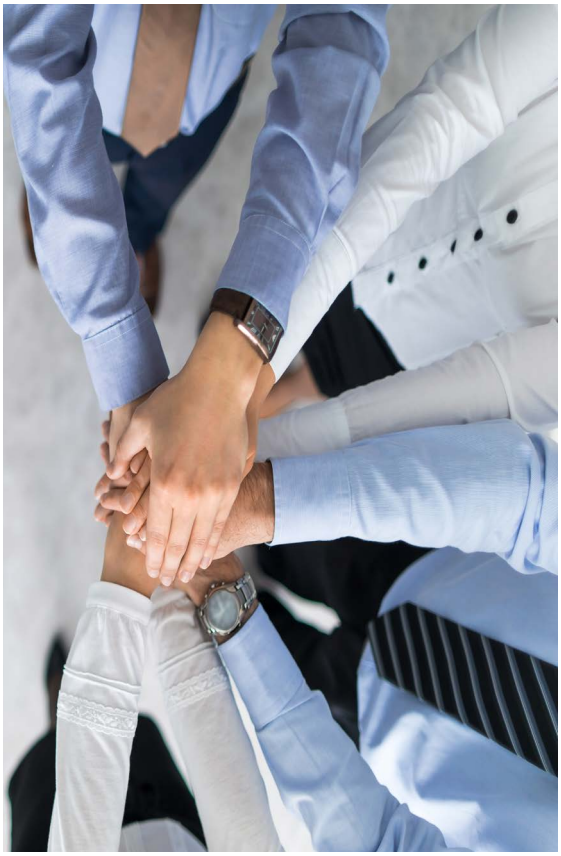


2.6. PUESTA EN MARCHA (FASE 6)

Una vez aprobado por la Dirección, el Plan Director de Seguridad marca el camino a seguir para alcanzar el nivel de seguridad que nuestra organización necesita. Como si de un proyecto más se tratara, cada organización puede emplear la metodología de gestión de proyectos que considere oportuno para llevarlo a cabo.

A continuación se indican una serie de aspectos cuya consideración favorecerá el éxito del proyecto y la consecución de los objetivos establecidos:

- Al inicio del proyecto, debemos llevar a cabo una **presentación general** del proyecto a las personas implicadas, haciéndoles partícipes del mismo e informándoles de cuáles son los trabajos y los resultados que se persiguen.
- **Asignar Responsables / coordinadores** de proyecto a cada uno de los proyectos establecidos y dotarlo de los recursos necesarios. Dependiendo de la envergadura del proyecto, puede ser necesario formar un Comité de Gestión que se encargue de la supervisión del mismo.
- Establecer la **periodicidad** con la que se debe llevar a cabo el **seguimiento** individual de los proyectos así como el seguimiento conjunto del Plan Director de Seguridad. Al respecto, cabe señalar que aquellos cambios en la organización o en el entorno de la misma que puedan modificar el enfoque estratégico, requerirán que revisemos igualmente el Plan Director de Seguridad, a fin de confirmar que sigue siendo válido y consecuente con la estrategia general de la organización.
- A medida que vayamos alcanzado los hitos previstos, debemos confirmar que las deficiencias identificadas en las auditorías o en el análisis de riesgos han sido subsanadas.



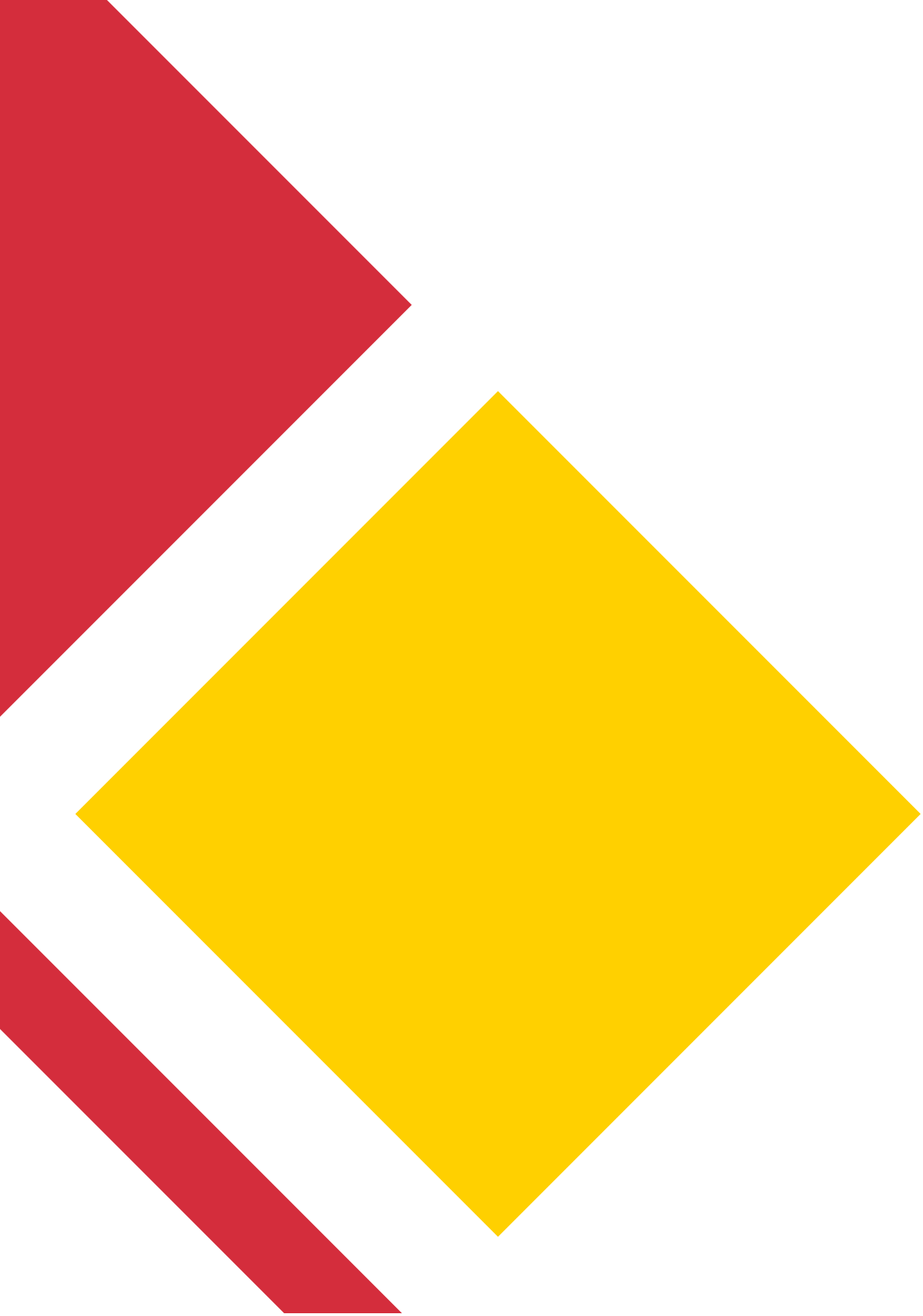
3. REFERENCIAS

[Ref - 1]. INCIBE, Copias de seguridad: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/copias-seguridad-guia-aproximacion-el-empresario

[Ref - 2]. UNE-ISO/IEC 27002:2015. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información - https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0055190

[Ref - 3]. INCIBE, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

[Ref - 4]. INCIBE, Guía de gestión de riesgos: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario



GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa