Plan director de seguridad

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. PLAN DIRECTOR DE SEGURIDAD

1.1. Antecedentes

En la actualidad la **información** se ha convertido en uno de los **activos más importantes** para las empresas, por lo que podríamos afirmar que estas basan su actividad en sistemas de información con soporte tecnológico. Por eso mismo debemos tener muy presente que **proteger la información** de la empresa es **proteger el negocio** y que es necesario llevar a cabo una gestión planificada de actuaciones en materia de ciberseguridad.

Un **Plan Director de Seguridad (PDS)** [1] está formado por un conjunto de proyectos que tienen como objeto el **reducir los riesgos** a los que está sometida nuestra empresa a unos niveles que consideraremos como **aceptables**.

Para poder desarrollar correctamente un Plan Director de Seguridad debemos partir de un buen análisis de la situación actual de la empresa. Además, nuestro plan tendrá que estar alineado con los **intereses estratégicos** de la empresa e incluirá las obligaciones y buenas prácticas que deberán cumplir todos nuestros empleados.

Una vez alcanzado un nivel de madurez adecuado podemos plantearnos, en función de la actividad de la empresa, el obtener una **certificación** que acredite nuestro sistema de gestión de la seguridad de la información.

1.2. Objetivos

Planificar los proyectos que queremos llevar a cabo a nivel técnico, organizativo y legal para **garantizar la protección de la seguridad de la información** de nuestra empresa, alineados con los intereses estratégicos de la organización.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **plan director de seguridad**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
A	PRO	**Analizar la situación actual de la empresa** Analizas detalladamente la situación actual de la empresa para poder acometer un Plan Director de Seguridad.	☐
A	PRO	**Alinear el PDS con la estrategia de la empresa** Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar el Plan Director de Seguridad.	☐
A	PRO	**Definir los proyectos a ejecutar** Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	☐
A	PRO	**Clasificar y priorizar los proyectos** Agrupas y clasificas las acciones a ejecutar con el fin de priorizar aquellas que nos proporcionen mayores beneficios en relación a su coste.	☐
B	PRO	**Aprobar el PDS** Apruebas y publicas la versión definitiva del PDS.	☐
A	PRO	**Ejecución del PDS** Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.	☐
A	PRO	**Certificación en seguridad** Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu empresa.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Analizar la situación actual de la empresa.** Formaremos un equipo para realizar un análisis detallado del estado inicial de la empresa en materia de ciberseguridad. Para ello tendremos en cuenta los siguientes aspectos:
  - **Actividades previas**:
    - acotar el alcance sobre el que se va a desarrollar el PDS, determinando que procesos, departamentos o sistemas son el objetivo principal de nuestro plan;
    - definir las responsabilidades sobre los activos, estableciendo para ello perfiles como el responsable de seguridad, responsable de información, responsable de ámbito, etc.;
    - realizar una valoración inicial de la situación;
    - analizar el nivel de cumplimiento actual de los controles del PDS, realizando reuniones, revisiones, inspecciones para determinar y evaluar el nivel de cumplimiento actual para cada control de seguridad;
    - establecer los objetivos a cumplir por la empresa en materia de ciberseguridad, seleccionando los ámbitos a mejorar e identificando los aspectos donde debemos centrar nuestros esfuerzos.
  - **Análisis técnico de seguridad**. Valoraremos el grado de implantación de ciertos controles de seguridad de los sistemas de información de la empresa. Tales como la disponibilidad de antivirus, cortafuegos, páginas web seguras, segmentación de red, controles de acceso físico, etc.;
  - **Análisis de riesgos**. También realizaremos un análisis de los riesgos a los que está sometida nuestra empresa, para ello seguiremos los siguientes pasos:
    - identificación de activos susceptibles de sufrir amenazas;
    - valorar los activos críticos;
    - analizar las principales amenazas que pueden sufrir nuestros activos;
    - medir las consecuencias de que un activo se vea afectado por una amenaza y estimar las probabilidades de que eso ocurra;
    - verificar las medidas de seguridad existentes que mitigan el impacto de las amenazas;
    - determinar los riesgos residuales a los que la empresa puede estar expuestos.

    Una vez identificados los riesgos, estableceremos el nivel de riesgo aceptable para la empresa que nos indicará que riesgos son asumibles y cuáles deben ser tratados y corregidos. Existen varias estrategias para gestionar los riesgos:
    - transferir el riesgo a terceros, lo más habitual en este caso es contratar de un seguro [2];
    - eliminar el riesgo (hacer esa actividad de otra forma que no tenga riesgo);
    - asumir el riesgo, pero siempre de manera justificada;

- implantar medidas para mitigar el riesgo.

- **Alinear el PDS con la estrategia de la empresa.** Para ajustar el PDS a las necesidades reales de la empresa lo alinearemos con la estrategia, teniendo en cuenta: las previsiones de crecimiento, los cambios debidos a reorganizaciones, si existe una estrategia de externalización, etc.
- **Definir los proyectos a ejecutar.** Tras analizar y valorar los riesgos y elegir la estrategia a seguir para cada uno, detallaremos las acciones concretas a ejecutar para alcanzar el nivel de seguridad acordado. Podrán existir proyectos de:
  - mejora en los métodos de trabajo actuales;
  - corrección de la ausencia o insuficiencia de controles físicos o técnicos;
  - gestión de los riesgos que tenemos que transferir o eliminar.

  Siempre tendremos en cuenta la viabilidad de estos proyectos dentro de nuestra empresa.
- **Clasificar y priorizar los proyectos.** Una vez identificadas las acciones concretas a llevar a cabo podemos agruparlas teniendo en cuenta diversos criterios, tales como su origen (si derivan de obligaciones legales, análisis técnicos, análisis de riesgos, etc.), el tipo de acción (técnica, organizativa, regulatoria, etc.). Tendremos en cuenta la identificación y priorización de aquellas acciones que requieran poco esfuerzo en su realización y cuyo resultado produzca mejoras sustanciales en la seguridad.
- **Aprobar el PDS.** Una vez disponible una versión preliminar del plan este deberá ser revisado y aprobado por la dirección. Una vez aprobada la versión definitiva del plan este se comunicará a todos los empleados.
- **Ejecución del PDS.** Tras la aprobación del PDS se comenzará su ejecución, ajustando su metodología de gestión a la empleada habitualmente por la empresa. Para favorecer el éxito en la consecución de los objetivos del plan consideraremos:
  - realizar una presentación general del plan a las personas implicadas;
  - asignar las responsabilidades para cada uno de los proyectos y dotarlos de los recursos necesarios;
  - establecer la periodicidad de revisión de cada proyecto y del plan en su conjunto, teniendo en cuenta que la aparición de cambios sustanciales en la empresa pueden obligar a revisar el plan en su totalidad;
  - según vayamos superando los hitos acordados, comprobaremos que las deficiencias localizadas han sido convenientemente subsanadas;
- **Certificación en seguridad**. Una vez ejecutado con éxito el PDS podemos considerar la obtención de una certificación que acredite la calidad de nuestra empresa en la gestión de la seguridad de la información. Esto es especialmente interesante si nuestra actividad está muy relacionada con las nuevas tecnologías. Podemos certificar nuestro sistema de gestión conforme a la ISO 27001 de Sistemas de gestión de la seguridad de la información [3].

  También podríamos considerar la adhesión de nuestra empresa a alguno de los **sellos de confianza** [4] disponibles en el mercado, que demuestren nuestro compromiso y buenas prácticas en materia de ciberseguridad.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plan Director de Seguridad https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

[2]. Incibe – Protege tu empresa – Blog – Pólizas de ciberriesgos: ¿Cuál me conviene? https://www.incibe.es/protege-tu-empresa/blog/polilzas-ciberriesgos-cual-conviene

[3]. AENOR – Certificación ISO 27001 de Sistemas de gestión de la seguridad de la información http://www.aenor.es/aenor/certificacion/seguridad/seguridad_27001.asp#.WMaOdvmgRJV

[4]. Incibe – Protege tu empresa – Sellos de confianza https://www.incibe.es/protege-tu-empresa/sellos-confianza

[5]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Continuidad del negocio https://www.incibe.es/protege-tu-empresa/herramientas/politicas

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD