Universidad Rey Juan Carlos

Ingeniería del Software

Ingeniería de Sistemas de Información

T1-EE3

Plan Director de Seguridad

A* Team

Carlos Solsona
Francis Cardi
Jesús Ortiz
Stefano Tomasini
Sergio Villagarcía

c.solsona.2020@alumnos.urjc.es

15 de octubre de 2023

Índice

1. Introducción

Vivimos en una era caracterizada por cambios vertiginosos, donde la tecnología y la interconexión global han revolucionado la operación de las organizaciones y las dinámicas sociales. En este contexto dinámico, la seguridad se ha consolidado como un pilar fundamental para empresas, entidades gubernamentales y cualquier institución que busca preservar la integridad de las personas, los activos, la información y los procesos. La imperante necesidad de salvaguardar estos pilares se ha convertido en una prioridad innegable.

En este escenario, el Plan Director de Seguridad (PDS) se erige como una herramienta crítica, meticulosamente diseñada para abordar de manera integral los desafíos y amenazas que enfrentan las organizaciones en pleno siglo XXI. El PDS no solo identifica y evalúa riesgos potenciales, sino que también establece medidas y procedimientos destinados a prevenirlos, atenuar sus consecuencias y garantizar la continuidad de las operaciones incluso en las circunstancias más adversas. Su alcance se extiende más allá de la mera seguridad física, abarcando la salvaguardia de información sensible y la ciberseguridad, aspectos críticos en un mundo donde los datos representan uno de los activos más valiosos.

A lo largo de esta introducción, nos adentraremos en los pilares fundamentales del PDS y su rol esencial en la protección de activos y el bienestar de la sociedad en su conjunto. Asimismo, subrayaremos su contribución en la creación de entornos seguros y resilientes, capaces de adaptarse a los desafíos cambiantes de un mundo cada vez más complejo y amenazante.

A medida que profundicemos en esta exploración, descubriremos cómo el PDS se erige como una herramienta insustituible para las organizaciones, permitiéndoles anticiparse a posibles amenazas, fortalecer su posición en el mercado y, en última instancia, contribuir a la edificación de un mundo más seguro y sostenible.

1.1. ¿Qué es un PDS?

Un Plan Director de Seguridad (PDS) es un documento estratégico y multidisciplinario diseñado para gestionar y garantizar la seguridad en una organización, entidad gubernamental o institución. Su principal objetivo es proporcionar una visión holística de las medidas y procedimientos necesarios para salvaguardar la integridad de las personas, los activos, la información y los procesos que forman parte de la operación de la entidad.

Este plan se ocupa de varios aspectos fundamentales de la seguridad. En primer lugar, identifica y evalúa los riesgos potenciales a los que la organización puede estar expuesta, ya sean riesgos físicos como robos o desastres naturales, o riesgos digitales relacionados con la ciberseguridad y la protección de datos sensibles. Luego, el PDS establece las estrategias y medidas necesarias para prevenir estos riesgos, o en caso de que ocurran, para mitigar sus impactos y garantizar la continuidad de las operaciones de la entidad.

El enfoque del PDS no se limita únicamente a la seguridad física, sino que se extiende a la protección de información confidencial y a la ciberseguridad. En un mundo donde la información es un activo crítico, el PDS se convierte en una herramienta esencial para salvaguardar los datos y sistemas de la organización, asegurando que estén protegidos contra amenazas digitales, como ciberataques y violaciones de la privacidad.

En resumen, un Plan Director de Seguridad es una guía estratégica que aborda de manera integral los desafíos de seguridad a los que se enfrenta una entidad en el entorno en constante cambio del siglo XXI. Su importancia radica en su capacidad para anticipar, gestionar y mitigar riesgos, contribuyendo a la protección de los activos y al bienestar de la sociedad en su conjunto.

2. Fase 1 - Conocer la situación actual de la organización

2.1. Actividades previas

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

Es la fase más importante del PDS debido a la importancia que tiene que la información necesaria para evaluar la situación actual sea fiable, completa y actualizada. En esta fase es fundamental contar con el apoyo de la dirección.

Sin embargo, antes de comenzar con los análisis, es necesario realizar algunas actividades previas:

2.1.1. Establecer el alcance

El alcance determinará la magnitud de los trabajos y también cuál será el foco principal de la mejora tras la aplicación del PDS.

Lo recomendable es determinar aquellos activos y procesos críticos, con los que la empresa sin ellos no puede subsistir, y usarlos como alcance del PDS.

2.1.2. Definir responsables sobre la gestión de los activos

Esto nos facilitará hacer un seguimiento tanto de la ejecución de las iniciativas planteadas como del análisis y recogida de la información.

Dichas responsabilidades deben estar asociadas a perfiles específicos. Se deben definir, al menos, los siguientes:

- Responsable de Seguridad
- Responsable de Información
- Responsable de ámbito (iniciativas en el ámbito legal, organizativo, etc.)

2.1.3. Valoración inicial

Se realizará una valoración preliminar de la situación actual de la organización para determinar los controles y requisitos que son de aplicación. Estas son las medidas 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 ISO/IEC 27002:2017, diseñada para ser utilizada a la hora de designar controles para la selección e implantación de un Sistema de Seguridad de la Información.

Después de analizar los controles, elaboraremos un documento con los controles o medidas de seguridad que apliquemos en la organización y su grado de madurez (en qué estado están).

Podemos partir de una escala de madurez de cinco niveles como la siguiente:

- Inexistente
- Inicial
- Repetible
- Definido

- Administrado
- Optimizado

2.1.4. Análisis de cumplimiento

Se deben realizar reuniones con el personal de los distintos departamentos de la organización para evaluar el cumplimiento de los controles de seguridad implantados. Es importante que la dirección traslade a cada una de las áreas la importancia del proyecto.

Registraremos todos los problemas y evidencias que vayamos detectando en relación con los requisitos de seguridad prefijados y una vez que dispongamos de toda la información, analizaremos los resultados.

2.1.5. Establecer los objetivos

Por último, se deben establecer cuáles son nuestros objetivos para 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.

2.2. Análisis técnico de seguridad

El análisis técnico de seguridad consiste en valorar el grado de implantación y madurez de los controles más relacionados con los sistemas de información.

En vez de evaluar el nivel de seguridad de la información de una organización basándonos en entrevistas y percepciones generales, el grado de seguridad de la información queda mejor evidenciado por aspectos técnicos concretos como:

- Si se tiene instalado en los ordenadores software antivirus que sea efectivo
- Si la página web está siendo mantenida a un ritmo razonable para que sea segura y se busquen y parcheen vulnerabilidades.
- Si la información crítica se encripta.
- Si se tiene puesto un cortafuegos, y este se configura bien.
- Si las contraseñas se guardan hasheadas en nuestra base de datos.
- Si se segmenta la red. Es decir, no se puede acceder desde fuera de la propia red de la organización a equipos o servidores internos.
- Si se sigue el principio del mínimo privilegio. Es decir, a cada empleado, según su rol, solo se le otorgan los permisos mínimos de acceso necesarios para que pueda realizar sus tareas efectivamente, en vez de dar permisos globales de acceso indiscriminadamente a todo personal.
- Si existen controles de acceso físico a áreas con información sensible, o crítica para el funcionamiento de la organización (salas de servidores, despachos, áreas de Recursos Humanos). O sea, que no se pueda robar/manipular cualquier tipo de información con tan solo ir en persona a usar los equipos.
- Si se limita el acceso a secciones críticas del sistema a un acceso físico/presencial si no es necesario en absoluto que estén conectadas a la red.
- Si existe un registro de acceso para aquella información sensible o crítica, en dónde tenga sentido que lo haya.

Las pruebas realizadas pueden ser de menor o mayor "agresividad", por lo que pueden afectar en diferente grado al funcionamiento de nuestros sistemas o redes durante su realización (mediante sobrecargas o de otras formas). Cabe limitar un sensible grado la "agresividad" de estas pruebas para no deshabilitar totalmente el funcionamiento de nuestro negocio, pero sin comprometer demasiado la efectividad del análisis. Deben establecerse procedimientos de recuperación al estado original del sistema antes de llevarlas a cabo, de lo contrario podría producirse una caída del servicio que tarde demasiado tiempo en arreglarse, y que suponga ser un considerable daño económico para la empresa al deshabilitar el funcionamiento del negocio.

Las auditorías técnicas deberían llevarse a cabo tanto desde el exterior de la organización como desde el interior de esta. Tomando el papel de distintos tipos de atacantes: tanto ciberdelincuentes ajenos a nuestra organización, como empleados nuestros descuidados, o malintencionados.

2.3. Análisis de riesgos

Hay que tener en cuenta que una organización no tiene a su disposición un presupuesto infinito para llevar a cabo un proyecto de ciberseguridad absolutamente exhaustivo de todos los riesgos existentes, todo esto conlleva un coste. Así que, toda organización sensatamente suele realizar un análisis de riesgos, para estudiarlos y priorizar solucionar aquellos que tienen:

- Un considerable impacto si se materializacen
- Una razonable probabilidad de que sucedan

...sobre aquellos que no tienen estos rasgos, o los tienen en menor medida.

Así que, paralelamente al desarrollo del análisis técnico de seguridad, se realiza este mencionado análisis de riesgos, que comprende la realización de las siguientes tareas:

- Se identifican y categorizan los activos de la empresa.
- De estos activos, se identifican cuáles son los más importantes de salvaguardar.
- Se listan todas las posibles amenazas que podrían materializarse sobre estos activos.
- Las amenazas listadas se priorizan según las consecuencias que tendrían sobre los activos que afectan si se materializacen, y también se estima la probabilidad de que suceda cada una. También se estiman los costes de producir la medida de seguridad adecuada.
- Después de haber implementado las medidas de seguridad que se consideraron necesarias, se estudian los riesgos residuales a los que la organización todavía podría estar expuesta.

3. Fase 2 - Conocer la estrategia de la organización

La fase 2 del Plan Director de Seguridad consiste en conocer la estrategia corporativa de nuestra organización.. Es importante considerar cualquier factor en relación a la empresa como, proyectos a futuro o una externalización de servicios TIC, ya que pueden llegar a afectar a la orientación de las medidas y al peso de cada una de ellas.

Esta fase tiene un menor peso en terminos de tiempo y esfuerzo en comparación con el resto, pero supone una parte fundamental de cualquier PDS, ya que nos permitirá implantar medidas de seguridad acordes a la naturaleza de la empresa.

Es fundamental alinear la estrategia de seguridad con la estrategia general de negocio de la organización, por ello, en esta fase se recomienda analizar la estrategia de la organización con los responsables de los departamentos implicados y con la Dirección para obtener una visión objetiva y global de la estrategia de negocio.

4. Fase 3 - Definición de proyectos e iniciativas

En este punto, debemos definir las acciones, iniciativas y proyectos necesarios para alcanzar el nivel de seguridad que nuestra organización requiere. Resulta fundamental considerar la estrategia de la organización a la hora de definir cualquier iniciativa.

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. Iniciativas dirigidas a mejorar los métodos de trabajo actuales
2. Acciones relacionadas con los controles técnicos y físicos cuya ausencia o insuficiencia hemos detectado
3. Estrategia a seguir, así como los proyectos más adecuados para gestionar los riesgos por encima de nuestro riesgo aceptable.

Un paso importante dentro de la fase será la estimación de coste de cada una de las iniciativas tanto en términos temporales como económicos.

5. Fase 4 - Clasificar y priorizar los proyectos a realizar

Después de identificar acciones, iniciativas y proyectos, es crucial clasificarlos y priorizarlos. Se sugiere agrupar iniciativas para homogeneizar el conjunto de proyectos. La clasificación puede basarse en el origen de las iniciativas y el tipo de acción. Independientemente de los criterios utilizados, es importante organizar los proyectos según el esfuerzo y el tiempo requerido, estableciendo proyectos a corto, medio y largo plazo. Además, se recomienda crear un grupo para iniciativas de "quick wins", aquellas que requieren poco esfuerzo pero generan mejoras sustanciales en la seguridad

6. Fase 5 - Aprobar el plan director de seguridad

En este punto, se ha desarrollado una versión preliminar del Plan Director de Seguridad, que debe ser revisado y aprobado por la Dirección. Durante la revisión, es posible que se realicen ajustes en el alcance, la duración o la prioridad de algunos proyectos. Este proceso de revisión puede repetirse ciclicamente hasta obtener una versión final formalmente aprobada por la Dirección.

Una vez que la versión final ha sido aprobada, se sugiere que la Dirección comunique y respalde el Plan a todos los empleados. Esto puede llevarse a cabo a través de reuniones o correo electrónico, destacando la importancia de la colaboración de toda la organización en la implementación del Plan Director de Seguridad.

7. Fase 6 - Puesta en marcha

Después de ser aprobado por la Dirección, el Plan Director de Seguridad guía el camino para alcanzar el nivel de seguridad necesario en la organización. Como un proyecto más, cada organización puede utilizar la metodología de gestión de proyectos que considere apropiada. Para garantizar el éxito del proyecto y la consecución de los objetivos, se destacan algunos aspectos clave:

1. Al inicio del proyecto, realizar una presentación general a las personas implicadas para informarles sobre los trabajos y resultados buscados, haciéndolos partícipes del mismo.

2. Asignar responsables/coordinadores a cada proyecto y proporcionar los recursos necesarios. Para proyectos extensos, se puede formar un Comité de Gestión para supervisar.

3. Establecer la periodicidad del seguimiento individual de los proyectos y del seguimiento general del Plan Director de Seguridad. Cualquier cambio en la organización o en su entorno que afecte al enfoque estratégico requerirá una revisión del Plan para confirmar su validez.

4. Conforme se alcancen los hitos planificados, confirmar la corrección de las deficiencias identificadas en auditorías o análisis de riesgos.