PLAN DIRECTOR DE SEGURIDAD (PDS)

ETAPAS DE UN PLAN DIRECTOR DE SEGURIDAD

1. Documentación y descubrimiento: ¿Cuál es la situación de ciberseguridad en nuestra organización? Es la primera pregunta que nos tenemos que plantear para poder construir un Plan Director de Seguridad exitoso. En colaboración con el personal de la empresa, y con la implicación imprescindible de la dirección, se conoce como se está operando con los activos de la organización (equipos informáticos, perimetrales, dispositivos móviles y aplicaciones) para evaluar la situación de partida. También se evalúa el valor de la información y los perjuicios que puede causar una parada inesperada en la continuidad del negocio, haciendo una valoración del coste empresarial en este escenario. Este descubrimiento es clave para la confección del PDS, proporcionando al técnico-auditor la visión necesaria para elaborarlo, acorde a las necesidades y carencias detectadas.

Un análisis de riesgos, del conjunto de amenazas y probabilidades de intrusión que nos permitan definir los objetivos que se quieren lograr, estableciendo las áreas de mejora y los puntos débiles a corregir

Como punto de partida de esta etapa definiremos 5 conceptos clave:

- El alcance de lo que vamos hacer determinando activos y procesos críticos.
- Los recursos humanos que van a participar en su elaboración
- La elaboración de un documento con la valoración inicial de la situación de la empresa relacionada con la seguridad de sus infraestructuras determinando el grado de madurez de la misma desde inexistente a óptimo.
- Elaboración de un inventario de equipos sensibles y cuáles son las medidas o aplicaciones de protección actuales.

2. ESTRATEGIA DE LA ORGANIZACIÓN

¿Cuál es el plan estratégico de la empresa en proyectos, crecimiento, cambios, etc.?
No podemos crear un PDS de corto alcance que suponga realizar inversiones ineficientes con un coste tanto económico como humano extra para la empresa.

En consecuencia, es necesario conocer los factores que pueden cambiar la situación actual de la organización para valorar cuales pueden afectar directamente a las directrices del PDS y cuáles no. En esta etapa toman especial relevancia las aportaciones de gerencia, dirección financiera y dirección TI, lo que nos permitirá tener una visión más amplia del camino que va a seguir la empresa en el medio-largo plazo.

¿EN QUÉ CONSISTE?

Todas las empresas, de todos los tamaños y en todos los sectores, son dependientes de los sistemas informáticos y de la información que en ellos guardan.

En algunos casos, a través de estas herramientas gestionamos información y procesos vitales para la compañía. Es decir, si dejaran de funcionar la actividad de la organización se paralizaría parcial o totalmente. Así pues, en estos y muchos otros casos es necesario implementar un Plan Director de Seguridad (PDS), que es, a grandes rasgos, un estudio del riesgo al que está expuesta la organización dada su dependencia de las nuevas tecnologías, en base al cual, se desarrolla un plan para reducir ese riesgo.

Un Plan Director de Seguridad expresa la estrategia de la organización en materia de protección de la Información, con el fin de diseñar, construir e implementar sistemas y procedimientos de seguridad, a fin de dar respuestas a incidentes informáticos o situaciones de riesgo inesperadas.

ABF CIBERSEGURIDAD y SISTEMAS

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Categoría MEDIA RD 3/2010

AENOR ER Seguridad Información UNE ISO/IEC 27001

3. Contenido: El documento elaborado recogerá las propuestas destinadas a la mejora de los procesos, siempre en el contexto en el que estamos actuando, las buenas prácticas en ciberseguridad.

Establecerá, de la misma forma, las acciones que se deben de tomar ante las insuficiencias detectadas y crearemos un nuevo marco de trabajo con los pasos adecuados para gestionar (y solucionar) los riesgos no aceptables por la organización.

Se cuantificará económicamente el coste de la adaptación en aquellas áreas afectadas que requieran intervención y se propondrán nuevos hábitos de trabajo que minimicen el riesgo de una brecha en la seguridad.

- **Plan de Contingencia y Continuidad de Negocio.**
  Busca proteger el funcionamiento normal de su empresa ante desastres o accidentes.

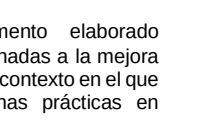
- **Adecuación a la RGPD.**
  Adecuar la organización al RGPD y en lo relacionado con la seguridad e integridad de los datos.

- **Política de copias de seguridad.**
  Es vital que se hagan copias de seguridad con frecuencia y regularmente. Es difícil la recuperación de la pérdida de datos si no se ha implementado una buena estrategia de copia de seguridad.

- **Regulación de servicios TIC con terceros.**
  La homogenización de servicios y productos con proveedores TIC externos con el fin de garantizar que cumplen con los requisitos establecidos en PDS para asegurar los protocolos de actuación aprobados.

4. Categorización y priorización: Una vez recogidas, en el PDS, todas las medidas y actuaciones a realizar para aumentar la seguridad de la organización, identificaremos las mismas priorizándolas por grado de amenaza, recomendando a la dirección de la empresa el proceso temporal de su ejecución y el coste, si lo tuviera, de llevarlo a cabo.

5. Aprobación del PDS: Versión final del Plan Director de Seguridad que será aprobado por la dirección de la empresa para su puesta en marcha de acuerdo al calendario establecido.



6. El PDS es el comienzo de un proceso de mejora continua en la organización relacionado fundamentalmente con la protección de la red informática y los datos que la misma contiene.

El resultado obtenido tiene que ser trasladado a toda la organización haciéndoles partícipe del mismo e informando de los objetivos que pretende. El plan debe de ser un elemento vivo que vaya evolucionando al compás de la empresa y que le ayude a marcar las normas y cultura corporativa.

Es recomendable la asignación de un responsable del proyecto en la empresa para que se encargue de la supervisión del mismo.

ABF CIBERSEGURIDAD y SISTEMAS

TELÉFONO: 941 10 70 80

info@abfsistemas.es

www.abfsistemas.es