

## ¿Cómo crear un plan de seguridad informática?

### 1. Identificación

Para proteger a tu organización, lo primero que debes hacer es saber lo que tienes en ella que vale la pena proteger. Este paso inicial implica averiguar el conjunto de los activos de la organización, incluido el personal, el hardware, software, sistemas y datos que componen tu sistema informático. Pueden incluir programas informáticos, servidores y servicios externos como alojamiento web.

### 2. Evaluación de riesgos

Ahora necesitas establecer qué es lo que podría poner en peligro los activos anteriores. Por ejemplo, los virus informáticos, hackers, daños físicos o errores de los empleados. Considera el tipo y el alcance del daño que podría ser causado en cada caso. Por ejemplo, si el servidor se pone fuera de línea, ¿tu empresa podría seguir funcionando?. Anota todo esto en tu plan de seguridad informática.

### 3. Prioriza tu protección IT

Una vez que hayas evaluado el daño potencial de cada amenaza y la probabilidad de que se produzca, puedes decidir qué amenazas son las más importantes e interesantes para empezar a proteger. Por ejemplo, podrías determinar que la protección de tu servidor es más importante que la protección de los equipos individuales.

### 4. Toma las precauciones adecuadas

Decide cuáles son los pasos que debes tomar para protegerte contra los riesgos que has identificado en toda la parte anterior de este plan de seguridad informática, y asegura que tu negocio va a seguir siendo capaz de operar si algo va mal. Por ejemplo, deberías restringir el acceso a tu servidor o instalar un firewall de hardware. Tu plan de recuperación de desastres debe explicar qué hacer si ocurre una crisis.

### ¿Que hacemos una vez tenemos el plan?

Una vez tengamos este **plan de seguridad informática** por escrito, debes poner en práctica las siguientes recomendaciones:

- **Comunica el plan a todo el personal:** Haz que algunos empleados concretos sean responsables de áreas específicas. Asegúrate de que tengan tiempo y recursos para hacer los cambios recomendados a sus sistemas de IT.
- **Crea políticas de IT y forma a la gente:** Modifica las políticas de IT para que estén en línea con el plan de seguridad. Si es necesario, forma a la gente para que todo el personal entienda cómo minimizar las vulnerabilidades de seguridad.
- **Establece un calendario para poner en marcha las medidas del plan:** Recuerda que puede tomar tiempo hacer grandes cambios en los sistemas.

### **Mantenimiento del plan de seguridad informática**

Los riesgos de seguridad cambian constantemente, por lo que deberás revisar periódicamente tu plan de seguridad informática. Mantente al día de las vulnerabilidades de seguridad emergentes suscribiéndote a boletines de empresas de seguridad. Asegúrate de que actualizas regularmente tus protecciones. Si se realizan cambios en tu sistema informático o inviertes en nuevo hardware o software, revise tu plan de seguridad informática. Tratar de identificar nuevas vulnerabilidades de seguridad y revisa también las políticas y procedimientos al menos cada 12 meses. Por último, pon a alguien a cargo del plan de seguridad informática, para que no haya ninguna posibilidad de que quede descuidado.

### **Referencias**

<https://www.universidadviu.com/crear-plan-seguridad-informatica-facilmente/>

<https://prezi.com/whxiuynnlfy5/ejemplos-de-politicas-de-seguridad-informatica-en-una-organizacion/>