Herramienta de autodiagnóstico

Consejos para un nivel **alto** de riesgo en **TECNOLOGÍA**

Su respuesta indica que aún no ha reconocido la importancia de fortalecer la ciberseguridad tecnológica en su negocio. El nivel de riesgo en ciberseguridad de su empresa en este aspecto ha sido considerado como **ALTO**. Eso significa que la probabilidad de que su empresa pudiera sufrir un ciberataque es muy alta. Le recomendamos que siga estos consejos:

- Si aún no lo ha hecho, considere implantar alguna **protección tecnológica** (*antimalware*, cortafuegos) como primer paso para proteger sus equipos. Y no olvide que el ***software* de seguridad** también tiene que estar **actualizado**.
- Revise quién puede entrar en sus dependencias y considere incrementar los **controles de acceso**. Los ataques a menudo combinan medios tradicionales con medios electrónicos.
- Si utiliza un servicio de **correo electrónico** gratuito para su actividad profesional quizá esté descuidando la seguridad que necesita su negocio. Valore contratar un servicio en el que tenga el control sobre su confidencialidad, integridad y disponibilidad.

Herramienta de autodiagnóstico

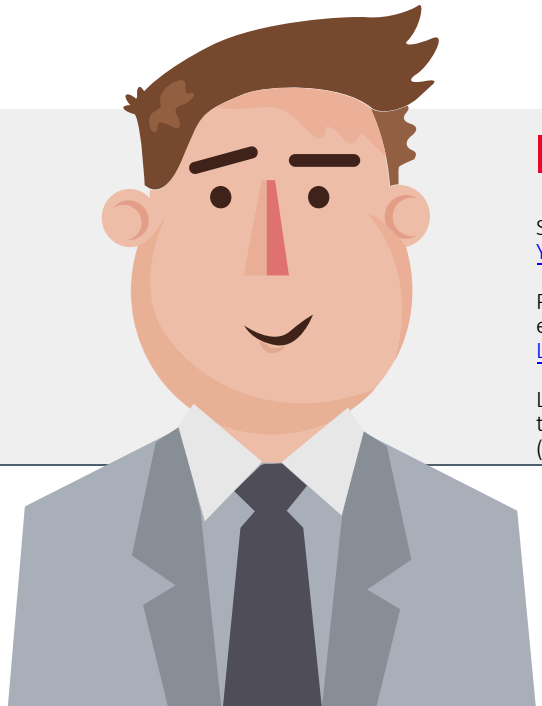
Consejos para un nivel **alto** de riesgo en **TECNOLOGÍA**

- Si dispone de **página web**, recuerde que tener al día el *software* de su página web es imprescindible pues muchos incidentes intencionados ocurren aprovechando vulnerabilidades del *software*. Además el daño causado por ese incidente puede ser grave y podría tener consecuencias legales si pierde datos personales de clientes. Revise este aspecto pues su página puede estar en riesgo.

- Si permite el **acceso remoto a sus sistemas**, no olvide tener un buen sistema de control de acceso virtual, monitorizarlo y tenerlo actualizado. **Formar a los usuarios y empleados** en su uso correcto es también muy recomendable.

- Si los **dispositivos móviles** son indispensables en su negocio considere contratar seguros o tener un plan B en caso de que se estropeen, pierdan o extravíen.

- Los ciberdelincuentes utilizan *malware* que ataca **sistemas no actualizados**. No actualizar esos sistemas, es como abrirles la puerta y dejarles robar datos o secuestrar sus sistemas. No debe permitírselo.



Información adicional

Si quiere más información, puede visitar la sección SECtoriza2 o el canal de empresas en Youtube.

Para estar al día, consulte nuestro blog, suscríbase a nuestros boletines o siga nuestros perfiles en redes sociales: Telegram @ProtegeTuEmpresa, Twitter @ProtegeEmpresa, Facebook o LinkedIn.

Le recordamos asimismo que para cualquier consulta se puede poner en contacto con INCIBE a través de la Línea gratuita de Ayuda en Ciberseguridad, 017; los canales de chat de WhatsApp (900 116 117) y Telegram (@INCIBE017), y el formulario de contacto para empresas.