Herramienta de autodiagnóstico

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

Sus respuestas indican que aún no ha reconocido la importancia de fortalecer el eslabón más importante de la seguridad, el empleado. 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 los siguientes consejos:

- **Forme a sus empleados** en seguridad de la información. La mayoría de los ataques aprovechan la falta de concienciación de los empleados.
- Si dispone de servidores de correo propios, recuerde que la administración de las **cuentas de correo** debería estar concentrada en una persona o un equipo. No es una buena práctica que cualquiera pueda hacerlo.
- Si dispone de **página web**, recuerde que actualizar los contenidos de la misma es una tarea delicada pues es el escaparate de su negocio. Por ello todos los responsables de hacerlo deberían ser personas de confianza. Es muy importante proteger sus credenciales de acceso, ya que si caen en otras manos puede ocasionar daños de imagen en su empresa.
- No hacer **copias de seguridad** o hacerlas sólo de vez en cuando no es una opción válida. Apunte en su agenda la planificación de estas copias de seguridad antes de que sea demasiado tarde.

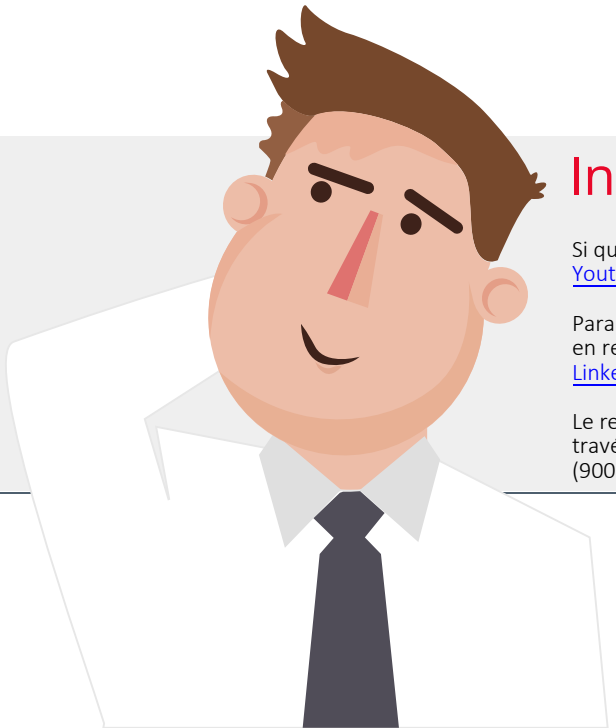
Herramienta de autodiagnóstico

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

- Las **cuentas de usuario con privilegios de administrador** tendrían que estar restringidas a las personas que estén autorizadas para este cometido. Si estas cuentas caen en manos de ciberdelincuentes podrían causarles graves daños a sus sistemas e incluso parar la actividad de su negocio…
- Si en su empresa los empleados pueden **acceder a aplicaciones internas desde el exterior** recuerde que este es un asunto delicado. Es necesario planificar los permisos de forma concienzuda y lo debe hacer una persona de confianza. Dejar esto en manos de todo el mundo no es una buena práctica.

- Si permite a sus empleados utilizar **dispositivos móviles** personales para uso profesional no olvide establecer y comunicar una política que indique los usos permitidos y no permitidos, y las medidas de seguridad que deben activar o contemplar (mantenimiento, actualización o sincronización).

- Considere **formar** a su personal informático en ciberseguridad o contratar **personal formado** en la materia.



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.