Herramienta de autodiagnóstico

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

Su respuesta indica que aún no ha reconocido la importancia de fortalecer la ciberseguridad en sus procesos de 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:

- Las **contraseñas** abren la entrada a nuestros sistemas y a nuestra información. La mayoría de los sistemas le permiten establecer reglas para su actualización periódica y para comprobar su fortaleza. No debe descuidar este aspecto.
- Un disco duro o un ordenador con información de carácter personal en manos de delincuentes puede causarle problemas legales y de imagen. No dude en establecer **políticas de destrucción de la información y los soportes.**
- El **correo electrónico** es un gran registro de nuestra actividad y la agenda donde tenemos los correos de nuestros contactos. Planificar las **copias de seguridad** es una buena costumbre.
- No es una buena práctica tener una **página web** y no realizar copias de seguridad. Tanto si la gestiona usted mismo como si lo tiene contratado, no olvide realizar copias periódicas.

Herramienta de autodiagnóstico

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

- Insistimos, no hacer **copias de seguridad** de la información en nuestros sistemas de forma regular no es una opción válida. Apunte en su agenda planificar estas copias antes de que sea demasiado tarde.

- Recuerde que incluso el correo electrónico de sus clientes es un dato personal protegido por el **RGPD** y que si utiliza la web para fines comerciales tiene que cumplir lo establecido en la **LSSI**.

- Si sus **servidores y routers** están en lugares de paso pueden sufrir por accidente o de forma intencionada alguna manipulación con consecuencias nada deseables. Considere cambiarlos de lugar a ser posible de acceso restringido.

- No es una práctica recomendable no tener un **plan B**. Incluso siendo previsores lo inesperado ocurre. El plan B nos va a dar la «resiliencia» necesaria para continuar a pesar de las contingencias.

- Si existen **teletrabajadores** en su empresa, cada día que, por accidente, estos no pueden realizar su actividad supone pérdidas. Tener un plan B garantiza que todo podrá salir adelante.

- Si **contrata servicios informáticos**, compruebe que los contratos contemplen las condiciones de ciberseguridad necesarias para hacer que su información esté segura. En particular si su empresa trata datos personales pues puede incumplir la LOPD.

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.