



Esta traducción se facilita a título informativo. Solo la versión alemana es jurídicamente vinculante. [Ver la versión alemana](#)

Formación y prueba de phishing: lo que nos espera

Información para toda la plantilla · Versión del 09.10.2026

En las próximas semanas haremos juntos una breve formación en línea sobre phishing y seguridad informática. Después llegarán al buzón algunos correos de phishing **simulados**, para que cada persona pueda poner a prueba con calma lo aprendido. Esta hoja explica qué ocurre y qué no ocurre en ningún caso.

¿Por qué lo hacemos?

El phishing es la vía más habitual por la que se ataca a las empresas: una factura falsificada, un supuesto mensaje del jefe, un «Su contraseña caduca». La tecnología intercepta mucho, pero no todo. El resto depende de nosotros. Además, las aseguradoras y los clientes exigen un justificante de que hemos recibido formación.

¿Cómo funciona?

- **Primero la formación:** Cada persona recibe un enlace al curso en línea. Dura aproximadamente una hora, a su propio ritmo, dentro del horario laboral.
- **Después la prueba:** Tras la formación, en el plazo de algunas semanas llegan algunos correos de phishing simulados. Parecen auténticos, pero son inofensivos.
- **Si hace clic:** Se abre una página explicativa que muestra en qué se podría haber reconocido la falsificación. Nada más. Un clic en falso es un momento de aprendizaje, no un fallo.
- **Certificado:** Tras la formación recibirá un certificado de participación personal.

Lo que ocurre

- La dirección ve una tasa del equipo («12 de 20 notificaron la falsificación»).
- Usted ve su propio resultado.
- Su nombre y su dirección de correo electrónico profesional se guardan para el envío y para el justificante de formación, en servidores ubicados en Alemania.

Lo que no ocurre

- Nadie recibe una lista de quién ha hecho clic.
- Nada pasa al expediente personal, a evaluaciones ni a conversaciones sobre el rendimiento.
- Ninguna exposición ante los compañeros, ningún «ranking».
- Ninguna supervisión del resto de su correo electrónico.

¿Qué debo hacer si un correo me parece extraño?

Exactamente lo que también sería correcto ante un ataque real: no hacer clic, no responder, notificarlo. Cómo y a quién se notifica se explica en la formación y vale tanto para los correos reales como para la prueba.

¿Preguntas? Persona de contacto en la empresa: · Comité de empresa:

La formación y la simulación las lleva a cabo secureIT UG (haftungsbeschränkt) por encargo de la empresa. Más información sobre el procedimiento y la protección de datos: secureit.icu/fuer-betriebsraete

