EMPRESARIOS

Buenas prácticas en redes sociales

básico

Contraseña de acceso robusta.

Como administrador de las redes sociales utilizas una contraseña fuerte y habilitas siempre que sea posible el doble factor de autenticación en todos los perfiles de la organización.

Configuración de privacidad.

Estableces la configuración de privacidad de manera que permita utilizar las distintas redes sociales de forma efectiva, permitiendo interactuar con el público sin descuidar la seguridad y privacidad del perfil empresarial.

Elegir un responsable de publicación.

Con esta acción evitarás la publicación de forma indiscriminada, además de disminuir el riesgo de sufrir un incidente de seguridad.

Definir unas normas de publicación.

Determinas la imagen que quieres reflejar, qué se publica y qué no, en qué tono o lenguaje, cómo se responde a las consultas de los clientes y a las quejas, etc., velando así por el perfil transmitido.

Estar al día de las amenazas.

Estás informado de las distintas campañas utilizadas por los ciberdelincuentes para conseguir acceso a los perfiles de las empresas en las distintas redes sociales.

Intentar evitar errores humanos.

Formas a los empleados en ciberseguridad para minimizar los riesgos relativos al uso de las tecnologías y, en particular, a las redes sociales.

Acciones a evitar.

A la hora de publicar usas el sentido común, teniendo en cuenta cómo puede afectar a la imagen de la empresa, evitando acciones como dar información confidencial, participar en discusiones, propagar noticias falsas, etc.

EMPRESARIOS

Buenas prácticas en redes sociales

avanzado

Restricciones de acceso.

Antes de conceder acceso u otro permiso a ciertas aplicaciones (de gestión, estadísticas, publicitarias, etc.), analizas detalladamente los riesgos que pueden suponer para tu perfil (acceso a información confidencial, publicaciones sin supervisión, etc.).

Precaución a la hora de seguir enlaces y descargar adjuntos.

Tratas los enlaces presentes en la red social y los documentos adjuntos con las mismas precauciones que en el correo electrónico. En caso de que un enlace te dirija a cualquier web que solicite cualquier tipo de información confidencial o bancaria, compruebas el certificado de seguridad y que corresponda con el sitio al que se está accediendo.