Buenas prácticas en redes sociales

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. BUENAS PRÁCTICAS EN REDES SOCIALES

1.1. Antecedentes

Hoy en día las redes sociales [1] se han convertido en una herramienta de marketing indispensable para las empresas. Más allá de la presencia general en la web, en las redes sociales es donde se configura la identidad virtual de la organización, y que puede utilizar para intentar ganar y fidelizar clientes, interactuando con ellos a través de estas aplicaciones. Una buena gestión de las redes sociales proporcionará visibilidad de la marca y sus productos, pudiendo atraer a una gran cantidad de público.

Hasta aquí todo parece positivo, pero debemos tener en cuenta que también se pueden convertir en un arma de doble filo si no tenemos en cuenta la ciberseguridad y, por tanto, no administramos de manera correcta el perfil empresarial, dañando así seriamente la imagen de la organización y, por ende, la confianza de los clientes.

1.2. Objetivos

- Garantizar la seguridad de los perfiles de las empresas en las redes sociales, evitando los incidentes de seguridad derivados de un uso carente de medidas de seguridad.
- Conocer las principales amenazas, malas configuraciones o fallos en su uso, que puedan afectar a la actividad, imagen y reputación de la empresa cuando se utilizan estas herramientas.

1.3. *Checklist*

A continuación se incluye una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **buenas prácticas en redes sociales**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO/PER	**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.	☐
B	PRO/PER	**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.	☐
B	PRO	**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.	☐
B	PRO	**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.	☐
A	PRO/PER	**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.).	☐

NIVEL	ALCANCE	CONTROL	
B	PRO/PER	**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.	☐
B	PRO	**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.	☐
A	PRO/PER	**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.	☐
B	PRO/PER	**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.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Contraseña de acceso robusta.** La contraseña es la llave de acceso a la red social, por lo que se debe utilizar una contraseña fuerte que no sea fácilmente descifrable, y habilitar siempre que sea posible el doble factor de autenticación [2]. De esta manera, además de tener que conocer el usuario y la contraseña para acceder a la cuenta, será necesario estar en posesión de un segundo factor, lo que aumenta considerablemente su seguridad. Un acceso no autorizado podría permitir el acceso a la configuración del perfil, comunicarse con clientes o publicar en nombre de la organización, lo que podría ocasionar fugas de información [3] y graves consecuencias para la reputación de la empresa.
- **Configuración de privacidad.** Todas las redes sociales cuentan con parámetros de privacidad que pueden ser configurados en un rango que va desde muy restrictivo a más laxo. La organización debe encontrar un punto intermedio que permita utilizar las distintas redes sociales de manera efectiva, de forma que permita interactuar con su público sin descuidar la seguridad y privacidad del perfil empresarial [4][5][6][7].
- **Elegir un responsable de publicación.** Si se permite que todos los empleados tengan acceso y publiquen de forma indiscriminada, la imagen de la empresa puede verse dañada, además de aumentar el riesgo de sufrir un incidente de seguridad [8].
- **Definir unas normas de publicación.** La organización debe definir la imagen que quiere 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. Descuidar estas normas puede influir negativamente en la opinión que los clientes se forman sobre la empresa.
- **Restricciones de acceso.** Existen ciertas aplicaciones que por ciertos motivos (de gestión, estadísticos, publicitarios, etc.) solicitan acceso y ciertos permisos en los perfiles de nuestras redes sociales, y que debemos analizar detalladamente antes de concederles estos privilegios. De lo contrario, esta práctica puede suponer un riesgo para la privacidad [9], ya que podría permitir el acceso a determinados datos (como información de seguidores o clientes), que deben ser privados, o permitir la publicación de contenido no supervisado por la empresa.
- **Estar al día de las amenazas.** La suplantación de clientes o proveedores y las campañas de *phishing* y *malware* [10] son los fraudes más utilizados por los ciberdelincuentes para engañar y extorsionar a las empresas a través de las redes sociales con el fin de obtener un beneficio económico. La suscripción al boletín de avisos de Protege tu empresa, de INCIBE, [11] te permite estar al día de las ciberamenazas que pueden perjudicar a tu organización, facilitando la prevención y protección ante el riesgo de sufrir un incidente de seguridad.
- **Intentar evitar errores humanos.** El desconocimiento y la falta de formación [12] en materia de ciberseguridad pueden llevar a una mala gestión de las redes sociales por parte de la empresa. Un error frecuente, y por tanto una práctica de riesgo, es la publicación de información privada, ya que los ciberdelincuentes utilizan estas aplicaciones como fuente de información. Publicar ciertos datos, como por ejemplo, la asistencia a un congreso o cualquier otra información relativa a la actividad diaria de la empresa, puede serles de gran ayuda a la hora de realizar estafas como el fraude del CEO [13].

- **Precaución a la hora de seguir enlaces y descargar adjuntos.** El *malware* también se difunde por las redes sociales mediante documentos adjuntos en mensajes dentro de la propia red o por medio de sitios web de terceros. Por lo tanto, debemos tratar los enlaces presentes en la red social y los documentos adjuntos con las mismas precauciones que en el correo electrónico [14]. En caso de que un enlace nos dirija a cualquier web que solicite cualquier tipo de información confidencial o bancaria, se comprobará también el certificado de seguridad y que corresponda con el sitio al que se está accediendo [15].
- **Acciones a evitar.** A la hora de publicar en las redes sociales debemos usar el sentido común, teniendo en cuenta cómo puede afectar a la imagen de la empresa y evitar acciones como:
    - Dar información confidencial o sujeta a propiedad intelectual.
    - Lanzar comentarios inoportunos, negativos o inapropiados, como por ejemplo, quejas laborales.
    - Emitir juicios de valor.
    - Enfrascarse en discusiones sin sentido, insultar, amenazar o acosar.
    - Propagar noticias falsas.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog – Día de los Tuiteros, comprueba la seguridad de las redes sociales empresariales https://www.incibe.es/protege-tu-empresa/blog/dia-los-tuiteros-comprueba-seguridad-las-redes-sociales-empresariales

[2]. Incibe – Protege tu empresa – Blog – Asegura tus cuentas de usuario con la autenticación de doble factor https://www.incibe.es/protege-tu-empresa/blog/asegura-tus-cuentas-usuario-autenticacion-doble-factor

[3]. Incibe – Protege tu empresa – Blog – ¡Fuga detectada, información robada! https://www.incibe.es/protege-tu-empresa/blog/fuga-detectada-informacion-robada

[4]. Instagram – Información y configuración de privacidad https://www.facebook.com/help/instagram/196883487377501

[5]. Facebook – Privacidad y seguridad https://www.facebook.com/help/1297502253597210

[6]. Twitter – Privacidad https://help.twitter.com/es/safety-and-security#ads-and-data-privacy

[7]. LinkedIn – Gestionar tu configuración de cuenta y de privacidad: resumen https://www.linkedin.com/help/linkedin/answer/555/gestionar-tu-configuracion-de-cuenta-y-de-privacidad-resumen?lang=es

[8]. Incibe – Protege tu empresa – Blog – Incidentes de seguridad, conoce a tus enemigos https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-conoce-tus-enemigos

[9]. Incibe – Protege tu empresa – Blog – Cómo proteger la información personal de los clientes en la empresa incibe.es/protege-tu-empresa/blog/proteger-informacion-personal-los-clientes-empresa

[10]. Incibe – Protege tu empresa – Avisos de seguridad https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[11]. Incibe – Suscripción a boletines de INCIBE https://www.incibe.es/suscripciones

[12]. Incibe – Protege tu empresa – Formación https://www.incibe.es/protege-tu-empresa/formacion

[13]. Incibe – Protege tu empresa – Blog – Historias reales: el fraude del CEO https://www.incibe.es/protege-tu-empresa/blog/historias-reales-el-fraude-del-ceo

[14]. Incibe – Protege tu empresa – Blog– Riesgos de abrir los archivos adjuntos de origen desconocido en el correo electrónico https://www.incibe.es/protege-tu-empresa/blog/riesgos-abrir-los-archivos-adjuntos-origen-desconocido-el-correo-electronico

[15]. Incibe – Protege tu empresa – ¿Qué te interesa? – Fraude y gestión de la identidad online https://www.incibe.es/protege-tu-empresa/que-te-interesa/fraude-gestion-identidad-online

INSTITUTO NACIONAL DE CIBERSEGURIDAD