

Perfiles corporativos en Redes Sociales.

Protección de la cuenta



Emplee contraseñas robustas para el acceso a las cuentas y renuévelas de manera periódica.



No abra desde sus redes sociales ningún enlace o fichero adjunto que presente cualquier indicio o patrón fuera de lo habitual, principalmente si se lo envía alguna persona desconocida.

Active la verificación en dos pasos. Establezca un segundo factor de autenticación (SMS, correo electrónico, etc.).



En caso de recibir un enlace acortado, se aconseja **emplear herramientas que permitan conocer la URL extendida** escondida.



Emplee una contraseña diferente para cada cuenta y red social, y no reutilice las contraseñas empleadas en otros sitios webs o recursos corporativos de su organismo o empresa.



Tenga especial cuidado con enlaces que reciba a través de mensajes directos, pues es uno de los principales vectores de ataque.



Habilite la opción de envío de alertas de inicio de sesión.



En caso de detectar una intrusión en alguna de sus cuentas en redes sociales, **notifique a la red social, cambie la contraseña de su perfil y denuncie** el caso a las Fuerzas y Cuerpos de Seguridad del Estado.



Debido a que las redes sociales actualizan rutinariamente sus configuraciones de seguridad y de privacidad, **verifique periódicamente el estado de su perfil** en ambas cuestiones.



No divulgue información personal en Internet que lo pueda vincular como gestor del perfil corporativo de una organización. En general, aplique sentido común.



