Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado

Estas directivas aplican a todas las cuentas de canales de comunicación oficiales del Estado: cuentas de redes sociales (Facebook, Twitter u otros), cuentas de correo electrónico institucional. En el caso de fanpage u otros canales oficiales gubernamentales que son administrados a través de cuentas particulares de funcionarios, éstas también deben cumplir estas directivas.

- Utilizar contraseñas robustas para las cuentas de correo electrónico y redes sociales: mínimo 12 (doce) caracteres, combinación de mayúsculas, minúsculas, números y símbolos
- Evitar utilizar contraseñas que sean fáciles de adivinar, no usar palabras comunes, fechas de cumpleaños, número de cédula o teléfono, nombres familiares, patrones de contraseña (ej.: nombre_institucion_año, nombre_cuenta_123, etc).
- Cambiar las contraseñas cada vez que hubiera un indicio o sospecha que éstas puedan haber sido comprometidas.
- No revelar las contraseñas a nadie, ni por correo, ni por redes sociales ni por teléfono.
- Utilizar autenticación de doble factor en las cuentas que lo permiten (Twitter, Facebook, Gmail, Outlook, etc.)

  Tutoriales:
  https://www.cert.gov.py/application/files/8914/3230/6320/Autenticacion_Doble_Factor.pdf
  - Twitter: https://help.twitter.com/es/managing-your-account/two-factor-authentication
  - Facebook: https://www.facebook.com/help/148233965247823?helpref=faq_content
  - Instagram: https://www.facebook.com/help/instagram/566810106808145?helpref=related
  - Mailchimp: https://mailchimp.com/es/help/set-up-a-two-factor-authentication-app-at-login/
  - Google (Gmail, GDocs, Youtube, etc.): https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=es-419
  - Outlook: https://support.microsoft.com/es-py/help/12408/microsoft-account-how-to-use-two-step-verification

- Vincular las cuentas oficiales de redes sociales a las cuentas de correo institucional de los administradores autorizados (.gov.py, .mil.py, o similar, según corresponda).
- Evitar usar cuentas compartidas, siempre y cuando la plataforma lo permita y sea posible. Cada administrador debe tener su propio usuario. Documentar claramente quién o quienes administran cada cuenta oficial.
  - Fanpage de Facebook: permite múltiples administradores a través de lo perfiles de Facebook individuales de cada administrador

  - Twitter: permite múltiples administradores, a través de TweetDeck
  - Instagram: permite un único administrador
  - Canal de Youtube: permite múltiples administradores a través de cuentas de Gmail individuales de cada administrador
  - Mailchimp: permite un único administrador
  - Cuentas de correo electrónico: siempre deben ser individuales

- Las cuentas de correo oficiales deben ser siempre individuales, debiendo cada usuario ser responsable del buen cuidado de su contraseña. En caso de requerir el uso de cuentas de correo electrónico genéricas, utilizar alias de correo siempre que sea posible.

- Configurar una contraseña de inicio de sesión y una contraseña de bloqueo de pantalla en todo dispositivo en la que tenga abiertas las cuentas oficiales (PC, teléfono, tablet).

- Verificar las cuentas oficiales de redes sociales, a través de los procedimientos establecidos por la Dirección General de Comunicación Estratégica del MITIC. Para ello, se debe cumplir con los requisitos establecidos en la siguiente guía: <link_a_guía>

- Si recibe una comunicación por correo electrónico o redes sociales que le solicita que ingrese la contraseña en algún formulario, tenga cuidado ya que podría ser una página falsa (phishing). Comprobar siempre la URL o dirección en la barra de direcciones del navegador y asegurarse de que se trate de la página real.

- En caso de sospecha de compromiso de una cuenta oficial, contactar de manera inmediata al responsable de Seguridad de la Información o de TICs de su institución o en su defecto al CERT-PY (MITIC), enviando un correo a abuse@cert.gov.py.

- En caso de suplantación de identidad de una cuenta oficial del Estado, debe reportarse directamente en la plataforma afectada, la cual actuará según sus términos y condiciones:

  - Twitter: https://help.twitter.com/es/safety-and-security/report-twitter-impersonation
  - Facebook: https://es-es.facebook.com/help/www/174210519303259?helpref=uf_permalink
  - Instagram: https://es-es.facebook.com/help/instagram/370054663112398?helpref=hc_fnav
  - Youtube: https://support.google.com/youtube/answer/2801947?hl=es-419