CIRCULAR Nº 03 /2021

EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (MITIC) recuerda y recomienda a los Organismos y Entidades del Estado (OEE) el uso de las **"Directivas de Ciberseguridad para canales de comunicación oficiales del Estado"**, aprobadas mediante la Resolución MITIC N° 432/2019, adjunta a la presente circular.

El objetivo de estas directivas es proteger las cuentas oficiales de comunicación gubernamental, resguardando no solo el acceso a las mismas, sino también el contenido de las comunicaciones asociadas a éstas. La protección inadecuada de las cuentas oficiales de comunicación del Estado puede comprometer la confidencialidad, integridad y disponibilidad de la información. Motivo por el cual, aplicando estas sencillas medidas recomendadas, colaboramos con la protección de las cuentas oficiales del Estado (página web, Facebook, Twitter, correo, etc.), evitando incidentes de seguridad.

Así también, medir el nivel de cumplimiento de estas Directivas permitirá una mejora continua en la definición de medidas de protección para actuar de forma proactiva, antes de presentarse cualquier incidente que ponga en riesgo la reputación, privacidad, información confidencial, etc.

En atención a ello, solicitamos completar la siguiente encuesta en: https://www.mitic.gov.py/encuestaecoe sobre las plataformas principales (página web principal, Facebook, Twitter, Instagram, otras cuentas oficiales), en forma obligatoria antes del 27 de agosto de 2021. La misma debe ser completada por el Responsable de Seguridad de la Información o en su defecto por el Director TIC, en coordinación con los funcionarios responsables de la administración de plataformas y/o redes sociales del área de Prensa/Comunicación de la Institución, quien deberá proveer la información necesaria para poder responder la encuesta.

Una vez culminado dicho periodo, el MITIC publicará un ranking de cumplimiento de todos los OEE, en base a los resultados recibidos. Se solicita además que estas Directivas puedan ser socializadas entre todos los funcionarios públicos o personas responsables de administrar una cuenta de comunicación oficial gubernamental.

Asunción, 07 de julio de 2021

Fernando Saguier Caballero Bernardes
Ministro - MITIC

PODER EJECUTIVO
MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

RESOLUCIÓN MITIC Nº 432.-

POR LA CUAL SE APRUEBA LAS DIRECTIVAS DE CIBERSEGURIDAD PARA CANALES DE COMUNICACIÓN OFICIAL DEL ESTADO.----------

Asunción, 04 de setiembre de 2019

VISTO: *El Memorándum DG N° 564/2019 de fecha 08 de agosto de 2019, de la Dirección de Gabinete del Viceministerio de Tecnologías de la Información y Comunicación de la Institución, a través del cual fuera solicitada la aprobación mediante acto administrativo de las Directivas de Ciberseguridad para Canales de Comunicación Oficial del Estado"; y,----------*

CONSIDERANDO: *Que, por Memorándum CyPI-20190402 de fecha 02 de abril de 2019, de la Dirección General de Ciberseguridad y Protección de la Información, mediante el cual fuera elevada una propuesta de "Directivas de Ciberseguridad para Canales de Comunicación Oficial del Estado", conteniendo la misma una serie de recomendaciones de seguridad orientadas a todos los funcionarios que administran redes sociales y/o canales de comunicación oficial del Estado, de modo a minimizar la probabilidad de incidentes cibernéticos.----------*

Que, por Memorándum DG Nº 551/2019 de fecha 01 de agosto de 2019, la Dirección de Gabinete del Viceministerio de Tecnologías de la Información y Comunicación, remitió la propuesta presentada por la Dirección General de Ciberseguridad y Protección de la Información a la Dirección General de Asesoría Jurídica, solicitándose un dictamen sobre el citado documento.----------

Que, por Dictamen Nº 145/2019 de fecha 05 de agosto de 2019, la Dirección General de Asesoría Jurídica se expidió sobre la propuesta de la Dirección General de Ciberseguridad y Protección de la Información, manifestando no encontrar reparos legales al documento y sugirió proseguir con los trámites para la emisión del acto administrativo.----------

Que, por Memorándum DG Nº 564/2019 de fecha 08 de agosto de 2019, la Dirección de Gabinete del Viceministerio de Tecnologías de la Información y Comunicación solicitó la elaboración del acto administrativo pertinente, a fin de aprobar las "Directivas de Ciberseguridad para Canales de Comunicación Oficial del Estado".----------

Que, de manera a prevenir incidentes cibernéticos de canales de comunicación oficial del Estado, teniendo en cuenta que, por el amplio alcance de los mismos estos podrían ser objetivos de ataques, corresponde aprobar Resolución mediante las "Directivas de Ciberseguridad para Canales de Comunicación Oficial del Estado", y difundir las mismas a todas las instituciones del Estado, a fin de que tomen conocimiento de las directivas oficiales por parte de esta Cartera de Estado.----------

Que, por Ley N° 6207/2018 se "...CREA EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y ESTABLECE SU CARTA ORGÁNICA", en su Artículo 7° reza: "Competencias. El Ministerio tendrá las siguientes competencias:... 23 – Ejercer como Autoridad de Ciberseguridad, y de prevención, gestión y control de incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional".----------

Que, por Decreto Nº 2274 de fecha 06 de agosto de 2019 "POR EL CUAL SE REGLAMENTA LA LEY Nº 6207, DEL 22 DE OCTUBRE DE 2019, «QUE CREA EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y SE APRUEBA SU CARTA ORGÁNICA», el cual, en su Capítulo IV "Ciberseguridad", reza: "Art. 43.- Prevención en materia de ciberseguridad. El MITIC implementará los mecanismos de monitoreo, gestión, coordinación y respuesta ante los incidentes cibernéticos y amenazas que pongan en riesgo el ecosistema digital nacional y fomentará las iniciativas que contribuyan a la prevención de los mismos....".----------

PODER EJECUTIVO
MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

RESOLUCIÓN MITIC Nº 432.-

POR LA CUAL SE APRUEBA LAS DIRECTIVAS DE CIBERSEGURIDAD PARA CANALES DE COMUNICACIÓN OFICIAL DEL ESTADO.----------

Que, el mencionado Decreto, en su Artículo 44 establece: "Reporte de incidentes cibernéticos. El MITIC es la autoridad de prevención, gestión y control en materia de ciberseguridad en resguardo del ecosistema digital nacional. Las Instituciones del sector público, están obligadas a comunicar y denunciar ante el MITIC todos los incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional, siguiendo las directrices y procedimientos que serán reglamentados por Resolución del Ministro..."; y, en su Artículo 45 expresa: "Políticas y normativas en materia de ciberseguridad gubernamental. El MITIC debe dictar las directrices, normativas y estándares en materia de prevención, gestión y control de incidentes cibernéticos y seguridad digital, que son de cumplimiento obligatorio por las áreas de TIC o sus equivalentes dependientes de las Instituciones del sector público... ".----------

Que, la Ley Nº 6.207/2018, en su artículo 8º, establece que el Ministro es la máxima autoridad institucional. En tal carácter es el responsable de la dirección y de la gestión especializada, técnica, financiera y administrativa de la Entidad, en el ámbito de sus atribuciones legales, asimismo, ejerce la representación legal del Ministerio.----------

Que, el Decreto N° 475/2018 nombra al señor Alejandro Peralta Vierci como Ministro de Tecnologías de la Información y Comunicación (MITIC).----------

Las disposiciones contenidas en la Ley Nº 6.207/2018.----------

***POR TANTO:** en ejercicio de sus atribuciones legales,----------*

EL MINISTRO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION,

R E S U E L V E:

Artículo 1º ***Aprobar** las "Directivas de Ciberseguridad para Canales de Comunicación Oficial del Estado", de conformidad a lo expuesto en el exordio, que como Anexo I forma parte integrante de la presente Resolución.----------*

Artículo 2º ***Encomendar** al Viceministerio de Comunicación la difusión de las Directivas aprobadas en el Artículo 1º de la presente Resolución a través de los medios de comunicación a su cargo.----------*

Artículo 3º ***La** presente resolución será refrendada por el Secretario General de la Institución.----------*

Artículo 4º ***Comunicar** a quienes corresponda, y cumplido, archivar.----------*

Rodrigo Sánchez Stark
Secretario General

Alejandro Peralta Vierci
Ministro

PODER EJECUTIVO
MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

RESOLUCIÓN MITIC Nº 432.-

POR LA CUAL SE APRUEBA LAS DIRECTIVAS DE CIBERSEGURIDAD PARA CANALES DE COMUNICACIÓN OFICIAL DEL ESTADO.----------

ANEXO I
DIRECTIVAS DE CIBERSEGURIDAD PARA CANALES DE COMUNICACIÓN OFICIAL 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 doce (12) 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.).*
- *No revelar las contraseñas a nadie, ni por correo, ni por redes sociales ni por teléfono.*
- *Cambiar las contraseñas cada vez que hubiera un indicio o sospecha que éstas puedan haber sido comprometidas.*
- *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 un único administrador.*
  - *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.*

PODER EJECUTIVO
MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

RESOLUCIÓN MITIC Nº 432.-

POR LA CUAL SE APRUEBA LAS DIRECTIVAS DE CIBERSEGURIDAD PARA CANALES DE COMUNICACIÓN OFICIAL DEL ESTADO.----------

- *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.*
- *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*