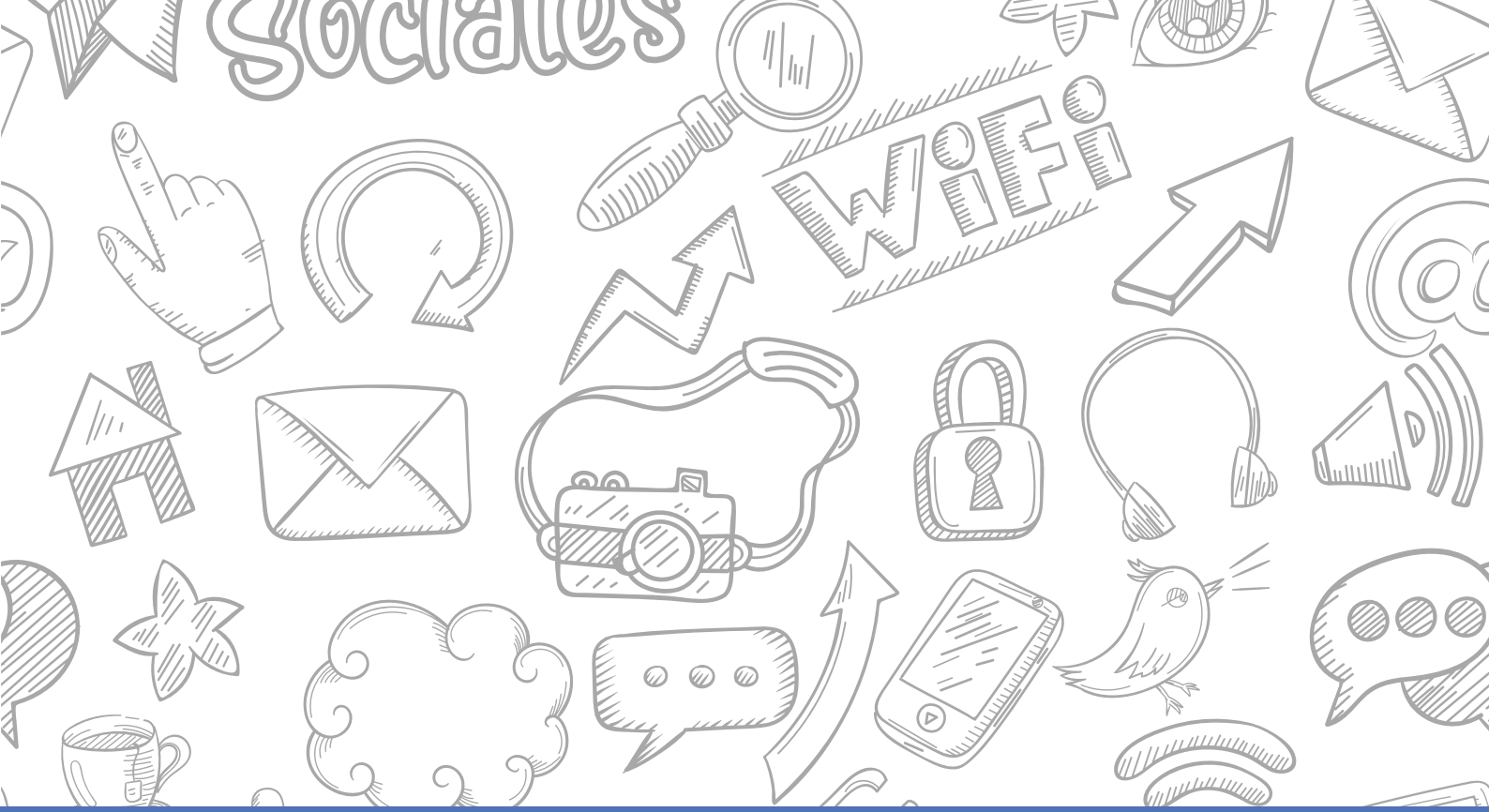
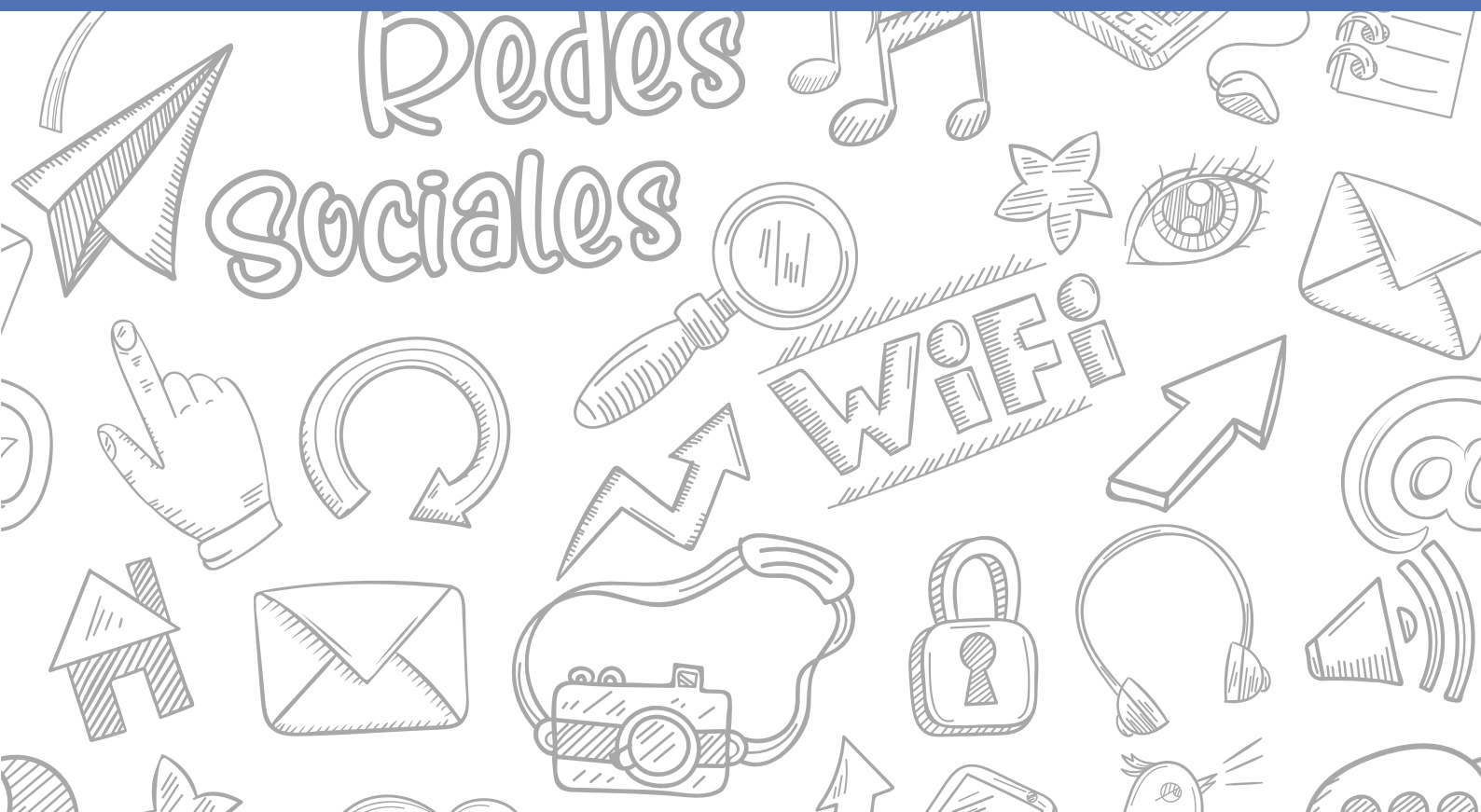


GUÍA PARA LA COMUNICACIÓN EN REDES SOCIALES DE ENTIDADES DEL PODER EJECUTIVO



CONTENIDO

GUÍA PARA LA COMUNICACIÓN EN REDES SOCIALES DE ENTIDADES DEL PODER EJECUTIVO

Guía para la Comunicación en Redes Sociales de Entidades del Poder Ejecutivo

INTRODUCCIÓN

Existe una gran cantidad de redes sociales útiles y necesarias para transmitir informaciones oficiales y relacionarse con públicos meta, las cuales se actualizan y modifican permanentemente. El Poder Ejecutivo, a través del Ministerio de Tecnologías de la Información y Comunicación (MITIC), entidad técnica e instancia rectora en cuanto a las Tecnologías de la Información y Comunicación en el sector público, así como de la comunicación del Poder Ejecutivo, pone a disposición la ***Guía para la Comunicación en Redes Sociales del Poder Ejecutivo*** con el objetivo de facilitar criterios y delineamientos básicos para el manejo de cuentas y/o perfiles de los Organismos y Entidades del Estado (OEE).

Este documento guía ofrece lineamientos, herramientas y ejemplos para la gestión diaria de contenidos en redes sociales desde las oficinas de comunicación, basándose en recomendaciones sencillas que buscan estandarizar el relacionamiento responsable y la comunicación transparente con la ciudadanía.

Las redes sociales son canales de comunicación multidireccionales que permiten conversar y gestionar las relaciones con la ciudadanía, la cual es considerada como un generador de contenido, debiendo ser respondido de forma oficial.

MITIC, Abril 2023

CONTEXTUALIZACIÓN

CONTEXTUALIZACIÓN

ACCESO A INTERNET EN PARAGUAY

La Encuesta Permanente de Hogares Continua[1], elaborada por el Instituto Nacional de Estadística (INE) reveló que el 77% de la población paraguaya, es decir 4 millones 526 mil personas, tenían acceso a Internet en el 2021.

Este estudio además evidenció que el 97,6% del total de la población de 10 y más años de edad, utilizó internet para mensajería instantánea (WhatsApp, Line), el 83,4% para redes sociales (Facebook, Twitter, Instagram) y el 83,0% para comunicaciones telefónicas.

A su vez, visibilizó que la mayoría de las conexiones a internet se realizaron desde un teléfono inteligente, para mayor precisión 9 de cada 10 personas accedieron a internet a través de un teléfono celular.

Esta información nos indica que la ciudadanía está conectada a canales de información las 24 horas, los 7 días a la semana.

[1] *https://www.ine.gov.py/news/news-contenido.php?cod-news=1169*

REDES SOCIALES MÁS UTILIZADAS A NIVEL MUNDIAL

Facebook, YouTube, WhatsApp, Twitter, Instagram, TikTok y LinkedIn son algunas de redes sociales más utilizadas a nivel mundial. Cada red social tiene una estética y uso particular, según sus características citamos algunas diferencias:

Facebook

- Por más de que permite redacciones extensas se recomienda no superar los 300 caracteres. Se recomienda iniciar el posteo con una breve descripción de un párrafo. Es conveniente el uso de fotografías y/o videos para ilustrar el contenido del cual se habla. Buscar siempre materiales de buena calidad y evitar fotografías y vídeos borrosos.
- Se recomienda un máximo de cinco posteos por cada día del Plan de Posteo. Hasta diez historias por día.
- Las publicaciones deben instar a la interacción y participación de los seguidores.
- Las publicaciones de relevancia para la institución pueden ser fijadas en el perfil el tiempo que se consideren sean necesarias de manera a otorgarles mayor visibilidad.
- Las historias deben estar en formato vertical para fotos y videos.
- Facebook permite mencionar a otras páginas o perfiles. En caso de compartir una información obtenida de otra fuente o autor que no sea propio, se debe mencionar a la fuente mediante las etiquetas o "@" arrobando, esto a su vez genera sinergia y colaboraciones. Esto para evitar reclamos posteriores por copyright.
- Se recomienda activar el Messenger, para recibir mensajes privados y brindar una respuesta en la brevedad.
- No se recomienda eliminar mensajes, es importante recibir la percepción e interacción del público.
- Utilizar "#*hashtags*" etiquetas, como máximo 4. Los hashtags ayudan a generar un álbum virtual de los temas generados bajo la etiqueta. Ejemplo: #Infome2023py. Buscando información bajo este #, se podrá visualizar todo lo publicado al respecto.
- Transmisiones de Facebook Live. Se recomienda informar con antelación sobre las transmisiones que se realizarán, mínimamente 1 día antes, así como 1 hora antes del inicio de la transmisión para recordar a la ciudadanía sobre la actividad. Acompañar con un flyer informativo con datos sobre ¿Qué actividad será? ¿Cuándo? ¿En qué horario? ¿En qué plataforma?

RECORDATORIO:
Es importante elaborar los posteos con información de calidad y corroborada. Calidad es mejor que cantidad.

Youtube

- Permite crear una cuenta/canal de YouTube. Una vez creado el canal se puede subir vídeos prácticamente en cualquier formato y a su vez compartirlo en otras redes sociales.
- Transmisiones de YouTube Live. Se recomienda informar con antelación sobre las transmisiones que se realizarán, mínimamente 1 día antes, así como 1 hora antes del inicio de la transmisión para recordar a la ciudadanía sobre la actividad.

Twitter

- Permite escribir mensajes cortos de hasta 280 caracteres). En Twitter Blue actualmente están habilitados hasta 4000 caracteres, como así también la función de editar tweet, cargar videos más largos (duración de hasta 60 minutos y con un tamaño máximo de 2 GB), tener una carpeta de elementos guardados.
- Permite incluir hasta 4 fotos, un archivo GIF o un video. A partir de una nueva actualización también está disponible la opción de compartir fotos, GIFs y videos en un mismo tweet.
- En caso de hablar de un tema extenso se puede utilizar el estilo “hilo de conversación”. En ese caso se recomienda indicar cada publicación de la siguiente manera: 1/3; “Parte 1”, “Parte 2”, etc.
- Se recomienda como mínimo 3 tweets al día y un máximo de 10 tweets por hora para no caer en el “spam”.
- No se recomienda @ arrobar a medios de prensa privados de manera constante, ya que puede ser considerado “*spam*” publicación no deseada. Hacerlo en casos sumamente urgentes y/o en necesidades de aclaratoria.
- Utilizar “*#hashtags*” etiquetas, como máximo 2. Los hashtags ayudan a generar un álbum virtual de los temas generados bajo la etiqueta. Ejemplo: #Infome2023py. Buscando información bajo este #, se podrá visualizar todo lo publicado al respecto.
- Incluir llamados a la acción como “Leé la entrevista completa” “Ayúdanos a difundir esta información”.
- Considerar la utilización de emoticones para transmitir emociones.
- Evitar las imágenes con mucho texto y los vídeos muy extensos.

RECORDATORIO:
Se recomienda retuitear publicaciones de importancia de otros perfiles institucionales.

Instagram

- Es una red social orientada a teléfonos móviles, también se puede visualizar en la versión web, aunque con mayores limitaciones.
- Se recomienda realizar un máximo de 5 posteos al día y un máximo de 10 historias.
- El tamaño recomendado para las publicaciones en Instagram es de 1080x1350 pixeles. En tanto para las historias de 1080X1920.
- Actualmente se pueden compartir en las historias videos de hasta 60 segundos sin corte. Desde el segundo 60 el material continúa en una nueva historia. Tienen una duración de 24 horas.
- En cuanto a los posteos de videos están los reels, que son videos verticales y pueden durar hasta 90 segundos. A diferencia de las historias, estas no se borran después de 24 horas, sino que permanecen en el feed una vez publicadas.
- Los vídeos con una mayor duración se suben también a la sección de Reels, luego de una última actualización de la aplicación.
- Utilizar "*#hashtags*" etiquetas, como máximo 7 y al final del posteo. Los hashtags ayudan a generar un álbum virtual de los temas generados bajo la etiqueta. Ejemplo: #Infome2023py. Buscando información bajo este #, se podrá visualizar todo lo publicado al respecto.
- El instagram *Live* permite realizar transmisiones en vivo desde teléfonos móviles para dar a conocer temas de interés de la institución y tener un contacto más directo e instantáneo con el público.
- Actualmente Instagram tiene la función *collab* que permite la colaboración de contenidos con otras cuentas. Es decir, dos perfiles pueden colaborar con una publicación que aparecerá en ambos feeds. Los likes, comentarios también se visualizarán de forma conjunta.
- Los comentarios que aporten un valor informativo o sirvan para generar interacción positiva pueden ser fijados en las publicaciones.
- Se recomienda que las historias que tengan relevancia para la institución o se consideren deben estar disponible para los seguidores sean agrupadas y fijadas en la parte superior del perfil con una portada en la sección de "Destacadas".

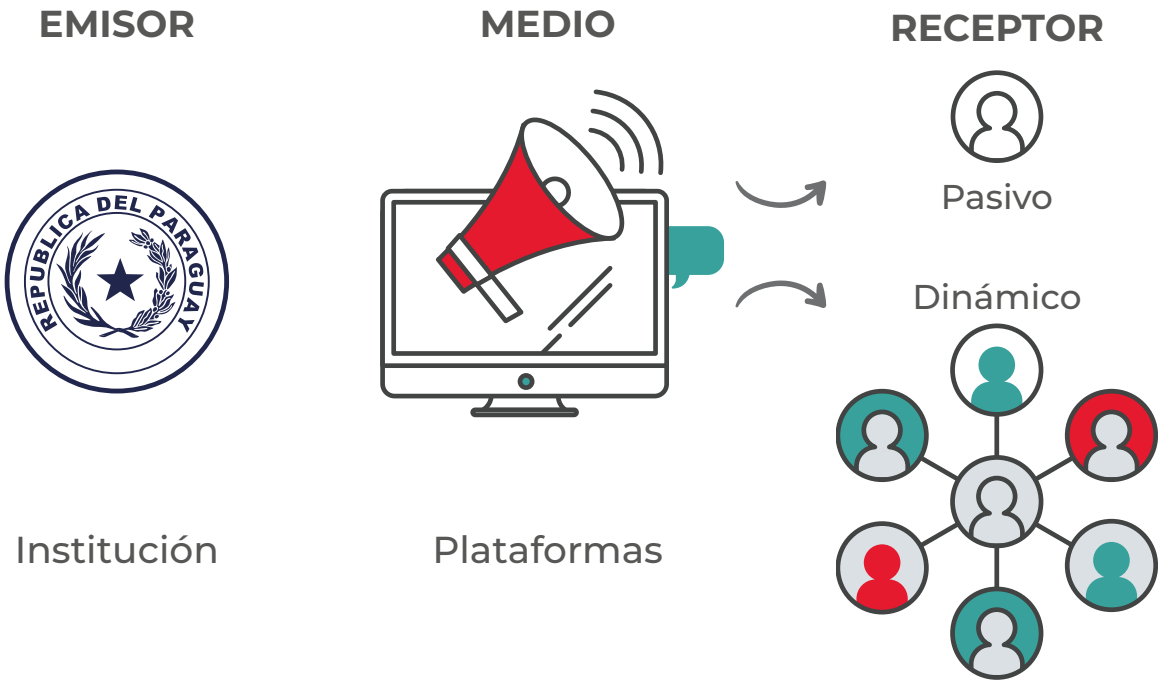
Linkedin

- Es una red social profesional, orientada a relaciones comerciales y profesionales más que a relaciones personales. Por tanto, en esta red social se encuentran empresas y profesionales que buscan promocionarse, hacer networking y negocios.
- Sirve para hacer publicaciones relacionadas a la búsqueda de personal (empleos ofrecidos) o para posicionar a empresas u organizaciones en sus rubros.

IMPORTANCIA DE LA COMUNICACIÓN DIGITAL PARA INSTITUCIONES DEL ESTADO: CONVERSACIÓN CON LA CIUDADANÍA

Las redes sociales y las plataformas digitales hacen que la comunicación sea multidireccional. El emisor (institución) emite el mensaje y la concepción actual en comunicación identifica al público como emisor ya que ofrece retroalimentaciones muchas veces de forma inmediata, con amplia capacidad de viralización o difusión.

Por ello las redes sociales deben ser vistas y manejadas como un canal de atención ciudadana; desde las instituciones se debe responder, orientar y/o derivar todas las consultas recibidas con celeridad, brindando un retorno en un tiempo no mayor a 24 horas.



OBJETIVOS Y ACCIONES DE LA COMUNICACIÓN DIGITAL DEL ESTADO

OBJETIVOS Y ACCIONES DE LA COMUNICACIÓN DIGITAL DEL ESTADO

Las cuentas oficiales de Entidades del Poder Ejecutivo, deben utilizarse teniendo presente los siguientes 5 objetivos comunicacionales:

a. Ser un canal y/o nexo de comunicación bidireccional entre el Gobierno y la ciudadanía

b. Posicionar a la Institución como primera fuente de información confiable y fidedigna para la ciudadanía en el rubro que le corresponde

c. Instalar los mensajes del Gobierno

d. Recibir la percepción ciudadana, y

e. Gestionar sus requerimientos e intereses, eficazmente.

La oficina de comunicaciones de las entidades debe funcionar como un espacio creativo y de desarrollo de contenidos oficiales que busquen lograr los 5 objetivos mencionados.

Para tener una buena administración de las cuentas es necesario:

a. Desarrollar el mensaje institucional sobre temas clave para la entidad.
b. Antes de abrir una cuenta o habilitar un perfil lo mejor es informase sobre cada una de las redes sociales para analizar cuál es la más conveniente de acuerdo a los objetivos de comunicación institucional. Por ejemplo, se puede utilizar una red para *educar*, otra para *informar* y otra para hacer una comunicación oficial institucional.
c. Actualizar diariamente las noticias, incluyendo logros del Gobierno, especificando el impacto positivo en la vida de las personas.
d. Desarrollar un listado de preguntas frecuentes, con respuestas pre-aprobadas por las autoridades de la institución.
e. Responder a los requerimientos de los/las usuarios/as (comentarios, sugerencias, denuncias/quejas) utilizando un lenguaje de cercanía, empático y respetuoso.
f. Desarrollar una Estrategia de Comunicación Digital con ejes de comunicación estratégicos para la institución (basada en el Plan de Comunicación Institucional)

METODOLOGÍA DE LA COMUNICACIÓN DIGITAL DEL ESTADO

ESTRATEGIA DE COMUNICACIÓN DIGITAL

Para comenzar a definir una estrategia es importante identificar los ejes estratégicos del Plan de Comunicación Anual, con los principales objetivos a los cuales la comunicación puede apoyar. Responder a las siguientes preguntas facilitará el desarrollo de la Estrategia de Comunicación Digital:

1. ¿Cuáles son los ejes acción de tu institución en los próximos 6 meses?. Considerar la visión, misión y el Plan Operativo Anual.
2. ¿Qué objetivos se desea lograr a través de las redes sociales?. La respuesta debe abarcar los **Objetivos y Acciones de la Comunicación Digital de Estado.**
3. ¿Cuál es el público al que se quiere llegar?
4. ¿Cuáles son las plataformas en redes sociales que mejor se adaptan a los contenidos que se desean transmitir?
5. ¿Quiénes estarán a cargo de la administración de esta(s) cuenta(s)?. Es importante definir roles para organizar correctamente el trabajo.
6. ¿Cómo deberá ser el flujo de información interno para mantener estas cuentas actualizadas a diario?

PLAN DE POSTEOS

En base a la Estrategia de Comunicación Digital que resulte de la respuesta a estas y otras preguntas, se debe consensuar un plan de posteos semanal. El mismo debe contemplar contenidos de gestión propia realizados de manera proactiva y planificada. Se deben planificar los trabajos del área para desarrollar creativamente contenidos sobre los avances y logros en el área misional, así como recordatorio de fechas importantes, preparando un breve texto informativo y un material audiovisual y/o gráfico.

Tener listo un plan de posteos actualizado y aprobado, será beneficioso para que el mensaje llegue de forma eficaz y eficiente, y para poder instalar la agenda institucional, evitando ser meramente actores reactivos a la agenda mediática y/o externa. (Ver ANEXO 1 Formato de Plan de Posteos)

PREGUNTAS CLAVE PARA EL DESARROLLO DE UN PLAN DE POSTEOS EFICIENTE

Para redactar un Plan de Posteos recurriremos a la Estrategia de Comunicación Digital y nos preguntaremos:

1. ¿Qué queremos transmitir?
2. ¿A quién o a quiénes servirá este contenido?
3. ¿Cómo debería presentarse el mensaje?
4. ¿A través de qué red social debería canalizarlo?
5. ¿En qué horario debería postearse para alcanzar al público meta y a la mayor audiencia posible?

Lo recomendable es desarrollar contenidos para cada red social y no postear en todo un mismo texto y/o imagen, puesto que cada una tiene sus características particulares y requiere de un recurso distinto para presentarse.

IMPACTO

Para tener un mayor impacto con las publicaciones institucionales se recomienda realizar reportes semanales y/o quincenales de tendencias de la audiencia de nuestras plataformas, identificando los contenidos de más éxito, los horarios de mayor interacción, así como las conversaciones que se posicionaron para poder actuar proactivamente realizando los ajustes correspondientes en los planes de posteos posteriores.

También es importante hacer un monitoreo constante de lo que se habla en las redes, y tener la capacidad de ajustar el plan en base al momento y al contexto. Una publicación en el momento inadecuado puede ser contraproducente e incluso generar una crisis, por más que el contenido haya estado bien trabajado.

LINEAMIENTO EDITORIAL INSTITUCIONAL

LINEAMIENTO EDITORIAL INSTITUCIONAL

TONO Y ESTILO EN PUBLICACIONES

Las cuentas en redes sociales se utilizan para comunicar, informar y educar a la ciudadanía, por lo tanto, la relevancia y el contexto para publicar son claves. Como voz institucional de gobierno debemos siempre mantener un tono respetuoso, amable y cercano. Es muy importante cuidar la gramática y la ortografía.

Un posteo debería llevar un máximo de 280 caracteres, imágenes de al menos de 800 pixeles. Podría estar acompañado de materiales audiovisuales de hasta un minuto en 720p. y usar dos hashtags que tengan relación al mensaje, la imagen debe contener la menor cantidad de texto posible.

Recomendado	NO recomendado
Iniciar con el saludo al realizar el primer posteo del día.	Utilización de memes.
Realizar una breve descripción de lo que se desea contar, complementaria a la imagen o video si los hubiere.	Utilizar un contenido compartido de otra página y no mencionar o @ la fuente.
Utilizar un lenguaje sencillo y respetuoso.	Responder de forma irrespetuosa a los comentarios.
	Eliminar comentarios.

Se recomienda

Se recomienda redactar guardando respeto a todos los usuarios de las redes sociales. Es de carácter reprochable en Internet y fuera de ella que una Institución del Gobierno realice comentarios despectivos u ofensivos.

Cabe recordar que cualquier actividad en la red queda registrada indefinidamente, accesible para cualquier usuario. No se recomienda borrar publicaciones realizadas, aunque podría haber excepciones según la situación. En lo posible se debe aclarar o corregir ya sea editando la publicación y/ o como un comentario, en el caso de un *"tweet"* se podría utilizar el formato de hilo.

RECOMENDACIONES

- Antes de publicar fotografías y/o videos se debe solicitar permiso a la(s) persona(s) que aparece(n) en ellos. Si se utiliza una imagen que no ha sido producida por el propio equipo de comunicación se debe identificar y reconocer el fotógrafo o realizador en la publicación original y publicar con los créditos correspondientes.
- Las imágenes deberán guardar relación con la información transmitida, preservando la privacidad y la dignidad de las personas, principalmente en caso de que aparezcan menores de edad.
- Recordamos que, de acuerdo a la Ley No. 433/2011, todo producto audiovisual lleve subtítulos; se recomienda incorporar además la lengua de señas.
- Todo contenido gráfico y audiovisual debe complementarse con su enunciado/texto de publicación. Se deben evitar repeticiones entre imagen y texto, o imágenes con texto insertado.
- No es adecuado utilizar las redes sociales institucionales para responder acusaciones o críticas realizadas hacia las autoridades de la institución.
- Las consultas realizadas a través de las redes sociales deben ser atendidas. Esta acción contribuye a que los seguidores se sientan escuchados y valorados. También sirven como evidencias para el sistema MECIP que promueve la apertura, transparencia y el diálogo con los ciudadanos.
- No se aceptan expresiones obscenas, vulgares ni en citas textuales.
- Se busca publicar contenido original (dar prioridad a campañas propias de la institución y pautas en tiempo real) y amplificar los mensajes prioritarios del Gobierno Central.
- Se debe priorizar el uso de las redes como un servicio público y masivo.
- El contenido publicado debe estar alojado en los sitios web correspondientes a cada institución/organización, para contar con mayor respaldo y credibilidad a la información entregada.
- La publicación de contenidos debe estar basada en el plan mensual de contenidos o aprobado por el Director General de las áreas de comunicaciones, prensa o similares.
- Las informaciones deberán ser claras, precisas y concisas, con un lenguaje sencillo y respetuoso.
- Los reposteos, reacciones (tales como “me gusta”, etc.) deben estar en concordancia con las líneas de comunicación oficial de los OEE. Se insta a realizar una verificación periódica de manera a evitar errores.
- Las etiquetas a otras cuentas deben estar en concordancia con el tema tratado.
- Las cuentas seguidas por el perfil institucional deben ser cuentas de Instituciones o personas referentes que aporten a la misión, visión y objetivos de los OEE.

ROL DEL COMMUNITY MANAGER (CM) O GESTOR DE COMUNIDADES

Es la persona encargada de crear perfiles y contenidos, gestionar la actualización de los mismos y dinamizar las comunidades de usuarios en Internet. El perfil de un/a CM de una plataforma gubernamental debe ser un punto intermedio entre estratega e implementador, por lo que requiere de ciertas habilidades técnicas y experiencia previa en el mundo digital. Esta persona puede y debe adaptar la estrategia entregada desde el Gobierno Nacional a su cartera buscando obtener una mayor eficacia.

Se recomienda que la persona que tenga este rol pertenezca al equipo interno de comunicaciones y/o prensa de la institución. Las cuentas no pueden ser manejadas por una autoridad o por personas externas.

Sus principales funciones son: generar una estrategia digital; desarrollar contenidos de acuerdo a la labor misional; plantear ideas creativas para insertar en los mensajes; generar una conversación y responder a las preguntas planteadas por los usuarios; hacer el seguimiento 24 horas 7 días de la semana a los perfiles institucionales en redes sociales.

Sus principales responsabilidades son: aplicar las directivas de seguridad de canales de comunicación del Estado, ingresar solamente desde dispositivos institucionales que cuenten con controles de seguridad básicos, abrir sesión y cerrar la sesión una vez finalizado el uso de las cuentas.

El trabajo de un/a CM debe ser complementado con el de un/a diseñador/a que pueda transformar la información estratégica en piezas visuales concretas y llamativas. En caso de no contar con un diseñador se recomienda la utilización de aplicaciones de diseño gráfico, como Canva (*www.canva.com*), siguiendo y respetando la línea gráfica institucional y la Norma de Gobierno.

RECOMENDACIONES GENERALES SOBRE REDACCIÓN

- Respetar las normas lingüísticas en los mensajes, los comentarios y las respuestas.
- Optar por textos breves que se puedan leer sin dificultad en los dispositivos móviles.
- Si la información necesita más caracteres, optar por más de una publicación (hilo, en el caso de Twitter).
- Cada vez que sea necesario y posible usar las menciones y etiquetas.
- En mensajes que lo necesiten usar con moderación los emojis y emoticones, según el estilo de comunicación.

CREACIÓN DE CUENTAS, PERFILES Y CANALES INSTITUCIONALES EN REDES SOCIALES

CREACIÓN DE CUENTAS, PERFILES Y CANALES INSTITUCIONALES EN REDES SOCIALES

REQUISITOS PARA LA CREACIÓN DEL PERFIL DE CUENTA OFICIAL INSTITUCIONAL

Para la creación del perfil de una cuenta oficial institucional se debe contar con la justificación, aprobada mediante documento firmado y sellado del Director General de Comunicaciones, prensa o similar del OEE solicitante. Ej.: Anexo 2 Formulario A

El documento de aprobación debe contener como mínimo la siguiente información para plataformas digitales:

- **Nombre descriptivo de la cuenta:** ej.“Ministerio de Prueba”
- **Nombre del perfil** y alternativa en caso de que el nombre ya se encuentre en uso: @mpruebapy / @mprueba_py. Se recomienda indicar el país con “py”
- **Cuenta de correo institucional asociada al perfil:** (solo institucional, no está permitido el uso de servicios de correo gratuitos como @gmail, @outlook, @yahoo, etc. que están fuera del control de la Institución dueña del perfil, tal como establecen las Resoluciones MITIC N° 432/2019 y N° 218/2020.
- **Número de teléfono asociado al nuevo perfil:** asegurarse que contenga un número de teléfono controlado exclusivamente por el Administrador. En caso de que la Institución cuente con un número de teléfono corporativo (móvil, línea alta o similar), se debe preferir éste como primera opción.
- **Nombre de la red social y/o plataforma digital:** (redes sociales, servicios de correo electrónico (solo para Google Drive), plataformas de servicios en línea, etc.) por ejemplo: Twitter, TikTok, gmail (solo para Google Drive), mailchimp, entre otros.
- **Adjuntar un plan de comunicación** digital orientativo para demostrar el tipo de contenido que desea difundir **(plan de posteo)**
- **Indicadores para medir gestión de las redes,** en caso de contar con Plan de Comunicación Institucional Anual.
- **Adjuntar los datos de los usuarios autorizados, sus roles y/o permisos de acceso.** Ej: Anexo 2. Formulario B. En caso que las personas designadas NO sean funcionarios en relación contractual directa con la institución (empresa o consultor tercerizado, voluntarios u otros) debe existir un contrato de confidencialidad. Asimismo, debe establecerse los términos y las condiciones de uso de las cuentas. En todos los casos, deberá indicarse a un funcionario de la institución como punto de contacto oficial.
- **Para las plataformas digitales** de comunicación diferentes a la de las redes sociales, debe verificarse, con el área de TIC del OEE, de no contar con plataformas y/o herramientas tecnológicas que brindan la funcionalidad requerida, con el fin de no duplicarlas.
- **Gestionar la verificación del perfil** para autentificar la veracidad de las cuentas y determinar que son los usuarios legítimos de los perfiles quienes la gestionan.

DESIGNACIÓN DE ADMINISTRADORES DE LA CUENTA Y COMMUNITY MANAGER (CM)

El Director General del área de comunicaciones, prensa o similar del OEE debe asignar mediante documento aprobado con firma y sello, a los funcionarios administradores de cuenta y community manager responsables de la gestión del nuevo perfil e informar el presente procedimiento para su aplicación.

DATOS DE IDENTIFICACIÓN DEL ADMINISTRADOR DE LA CUENTA

(Persona autorizada en disponer del control de los perfiles en plataformas digitales)

- Nombre y Apellido.
- Cédula de identidad civil.
- Correo electrónico institucional.
- Número de celular.
- Dependencia.
- Tipo de vínculo con la Institución: permanente, contratado, comisionado (indicar institución de origen).
- Perfiles o Cuentas autorizadas.
- Rol.

DATOS DE IDENTIFICACIÓN DEL COMMUNITY MANAGER

(Persona encargada de operar los perfiles de cuentas oficiales institucionales en plataformas digitales)

- Nombres y Apellidos.
- Cédula de Identidad Civil.
- Correo electrónico institucional.
- Número de celular.
- Dependencia.
- Tipo de vínculo con la Institución: nombrado, contratado, comisionado (indicar institución de origen), tercerizado (indicar razón social de la empresa).
- Perfiles o Cuentas autorizadas.
- Rol.

No se permitirá el acceso como **Administrador de Cuenta** a personas ajenas a la institución. No se permitirá que oficialmente se designe a personas ajenas a la institución, como responsables del contenido de la cuenta (Administrador de Cuenta) aunque se decida la tercerización de los servicios (Community Manager) se deberá identificar al responsable de la revisión de los contenidos a nivel institucional.

En caso que el Community Manager no sea personal con relación jurídica laboral directa con la Institución, deberá existir un contrato de confidencialidad y los términos y condiciones de uso de la cuenta. En todos los casos, deberá estar designado un personal de la Institución como responsable y punto de contacto.

RESPONSABILIDADES DEL ADMINISTRADOR DE CUENTA

- Dar de alta o baja la cuenta, realizar modificaciones en la administración de la cuenta, previa autorización del Director General de Comunicaciones, prensa o similares de los OEE.
- Conocer y aplicar las directivas de seguridad de cuentas oficiales y otras, si hubiere y velar por el cumplimiento de las mismas por parte de los usuarios de las cuentas oficiales.
- Ser el punto de contacto oficial para cualquier gestión de la cuenta ante el MITIC.
- Proponer la designación de una persona que se desempeñará como Community Manager (CM), y una vez aprobada su designación, asignarle los permisos de acceso a la plataforma (consultar documentación de la plataforma requerida).
- Asegurarse que el CM esté en conocimiento de las directivas de seguridad de cuentas oficiales y otras, si las hubiera; así como de velar por el cumplimiento de las mismas.
- En ningún caso se permitirá el uso de cuentas compartidas.
- Supervisar las actividades del Community Manager.
- Presentar el plan de contenido mensual para la gestión estratégica de la cuenta al Director General de Comunicaciones, prensa o similar para su aprobación.
- En caso de cambio del administrador de cuenta, la persona sustituida deberá entregar las credenciales (usuario y contraseña), métodos de validación para verificación de doble factor, al Director General de Comunicaciones, prensa o similar o al nuevo administrador designado por este. El nuevo administrador deberá:
    1. Cambiar las contraseñas.
    2. Designar los nuevos roles o permisos de ser necesario.
    3. Cerrar todas las sesiones abiertas.
    4. Actualizar el correo electrónico y teléfono asociado (si es que aplica).
- En caso de sustitución del administrador de la cuenta y/o CM, dar de baja al usuario de las plataformas digitales de la Institución.
- Ingresar solamente desde dispositivos institucionales que cuenten con controles de seguridad básicos. Caso contrario, si se utilizan dispositivos personales para el acceso, asegurarse de contar con controles de seguridad básicos: sistema operativo, navegadores y plugins (extensiones) actualizados, antivirus instalado y actualizado, contraseñas robustas para acceder al dispositivo, etc.
- En caso de incidentes de seguridad en la cuenta, reportar el incidente de acuerdo con los lineamientos de las Resoluciones MITIC N° 432/2019 y N° 346/2020 (ver enlace en la sección “Documentos de Referencia”) y/o consultar inmediatamente las recomendaciones de la plataforma afectada y realizar los pasos indicados.

CUENTA OFICIAL DE AUTORIDADES

En caso de que la autoridad ya cuente con perfiles de redes sociales, debe realizar los ajustes necesarios para la seguridad del perfil de acuerdo con las Directivas de Seguridad para Canales de Comunicación del Estado.

Es responsabilidad de la Dirección General del área de Comunicaciones, prensa o similares de la Institución informar a la Máxima Autoridad Institucional (MAI) acerca del uso permitido de la cuenta oficial como autoridad de la Institución.

En caso necesario, la autoridad puede solicitar asesoramiento a la Dirección General del área de comunicaciones, prensa o similares de la Institución o la Dirección de Medios Digitales del MITIC (*mediosdigitales@mitic.gov.py*), para comprensión de pasos que debe realizar en línea de forma particular (desde cada perfil) y/o en casos de pérdida de cuenta.

Se recomienda la verificación del perfil para autentificar la veracidad de las cuentas y determinar que son los usuarios legítimos de los perfiles los que las gestionan.

CREACIÓN DE CUENTA OFICIAL INSTITUCIONAL DE APOYO

Se recomienda que los Ministerios, Secretarías y Entes Autárquicos cuenten con un solo perfil, página o canal por red social, evitando generar varios, como, por ejemplo: Ministerios, Viceministerios y Direcciones Generales. Idealmente ese único perfil debe ser el de la institución paraguas. Poniendo como ejemplo el caso del MITIC, se debe tener sólo un perfil en Facebook/Twitter/Instagram, el cual debe ser el del Ministerio de Tecnologías de la Información y Comunicación propiamente dicho, no así de cada viceministerio ni de cada Dirección General o Dirección.

En el caso de la creación de una nueva cuenta para programas, campañas públicas o sub-unidades, es importante analizar la pertinencia comunicacional e informar al MITIC. Si la institución ya tiene implementada una cuenta oficial institucional que cumple con los requerimientos anteriores, justificar la creación de un nuevo canal institucional, respondiendo las siguientes preguntas:

¿A qué público se desea llegar, que no esté incluido en nuestro canal institucional ya vigente? ¿Cuál sería el período (inicio y fin) en el cual se debería mantener el nuevo perfil? ¿Cómo se trabajará a nivel institucional para coordinar que los contenidos en diversos canales, se comuniquen oficialmente en el mismo lenguaje o conceptos? Si se posee un plan de posteo básico, verificar que se definan los objetivos del nuevo perfil, principales líneas temáticas o contenidos e indicadores para evaluación de la gestión.

Una vez completada la justificación, la creación y asignación de personal autorizado deberá seguir los mismos pasos para la creación de una cuenta oficial institucional principal.

Todas las cuentas deben ser creadas con correos institucionales y seguir las buenas prácticas de ciberseguridad emitidas por el CERT Py (*www.cert.gov.py*) dependiente del MITIC (Ver ANEXO 3, Resumen de recomendaciones emitidas por CERT Py).

Las cuentas institucionales, las de apoyo y aquellas pertenecientes a las Máximas Autoridades Institucionales deben ser verificadas para autenticar la veracidad de las cuentas y determinar que son los usuarios legítimos de los perfiles los que las gestionan.

BAJA DE CUENTAS OFICIALES INSTITUCIONALES

Los perfiles de cuentas oficiales institucionales (principal o de apoyo) deben ser archivados y las informaciones de los perfiles permanecer disponibles, previo cambio de las contraseñas, en los siguientes casos:

- La Institución deje de existir (fusión, supresión, otro)
- Finalización del programa comunicacional que motivó la creación de la cuenta.

En caso de que la plataforma no permita archivados, asegurar el resguardo de la información. El resguardo de la información será responsabilidad de la persona que se encuentre ejerciendo la Dirección de Comunicación al momento de la ejecución.

En caso de que las Instituciones se renombren y/o se produzcan cambios de administración, deberán seguir utilizándose los perfiles oficiales, ajustando la configuración y/o descripción conforme a los nuevos lineamientos de imagen o comunicacionales, si lo hubiera.

En cualquiera de los casos, ante la desvinculación del responsable institucional de la cuenta, el administrador de la cuenta o su equivalente designado es el responsable de gestionar dichos pasos.

GESTIÓN DE CRISIS Y EMERGENCIAS

GESTIÓN DE CRISIS Y EMERGENCIAS

Crisis: Existen varias definiciones, pero tomaremos como base la siguiente: todo evento inesperado (o indeseable) que amenaza la imagen y reputación de una institución y que tiene el potencial de generar un alto impacto negativo o una percepción inadecuada de los hechos en un público amplio o en un sector de alto interés institucional.

Las crisis en redes sociales tienen particularidades propias: se dan en tiempo real; se pueden amplificar rápido; los comentarios y reacciones de los usuarios no son controlables.

Emergencia: Situaciones de riesgo colectivo de origen natural o provocado por la acción humana.

¿CÓMO PROCEDER ANTE UNA CRISIS O EMERGENCIA EN REDES SOCIALES?

Se recomienda evitar la proactividad y la improvisación. Si no se está seguro de la información que se plantea publicar, la sugerencia es la abstención hasta tener la confirmación y recién allí hacerlo. La comunicación en redes sociales en periodos de crisis y emergencia es muy importante ya que es una herramienta de información para los ciudadanos. Toda la comunicación debe ser oficial y debe ser validada previamente y contar con una fuente confirmada.

Ante una crisis o emergencia recomendamos informar de inmediato al MITIC para asegurar una respuesta coherente y consistente, acorde con los lineamientos del Gobierno Nacional.

Dependiendo de la gravedad de la crisis se recomendará la creación de un gabinete de crisis que determinará en Plan de Acción, el cual incluirá quién, cuándo, dónde y cómo se responderá. Se recomienda recopilar de inmediato toda la información que hace a la crisis y coordinar con las áreas afectadas, incluyendo la asesoría jurídica. Se debe tener en cuenta que hay veces en que es más importante saber administrar una publicación negativa y sus impactos, antes que responder a la misma.

En el Plan de Acción se debe incluir a los Medios del Estado, un soporte válido para dar la información oficial en respuesta a situaciones de crisis.

En momentos de crisis o emergencias los contenidos que no tengan que ver con la contingencia deben ser pospuestos.

ELEMENTOS QUE PUEDEN GENERAR O AGRAVAR UNA SITUACIÓN DE CRISIS O EMERGENCIA:

• **Comentarios negativos o de información falsa:**
Ante este tipo de posteos se recomienda responder brindando información fidedigna, incluyendo "links" (vínculos) de publicaciones con mayor información sobre el tema referido. No es recomendable responder a críticas mal intencionadas, así como, comentarios irrespetuosos o de lenguaje inapropiado.

• **Los llamados *"Trolls":***
Un ***"troll"*** es un usuario de identidad desconocida y poco fiable. En ese caso, según la plataforma correspondiente (twitter, Facebook, Instagram, YouTube. Etc.), puede ser denunciada la cuenta e incluso recomendamos ocultar dichos comentarios ya que pertenecería a un usuario sin identidad comprobable.

• **Los llamados "Haters" en redes sociales:**
Los ***"haters"*** son perfiles que realizan críticas malintencionadas, o denuncias varias. En estos casos no se recomienda responder de forma rápida e impulsiva a las acusaciones/argumentaciones. Es necesario contar con una estrategia y responder solamente si se cuenta con argumentos fuertes y fidedignos para ello. Recomendamos comunicar al superior inmediato sobre la situación y entablar una comunicación inmediata con el punto focal del MITIC para establecer los lineamientos de respuestas en situaciones de crisis.

Es importante verificar/investigar el perfil de las cuentas que realizan críticas y/o comentarios ofensivos. Es importante hacer el seguimiento y sobre todo prestar especial atención a los generadores de contenido que tienen impacto, y ser hábiles en identificar a los nuevos haters que puedan nacer a partir de ellos. Se debe estar atento y tener respuestas rápidas y preferentemente indirectas a sus ataques.

Se recomienda además aplicar los **filtros de groserías** ya sea al crear el perfil y/o al actualizarlo en ***Configuración de la página General Filtro de Groserías Moderado/Elevado.*** Con esto se busca evitar palabras irrespetuosas y administrar mejor las interacciones de perfiles probablemente falsos.

LA EVALUACIÓN POSTERIOR A UNA CRISIS

Pasado el episodio negativo es importante realizar una evaluación crítica de las acciones realizadas, para poder en próximas ocasiones repetir lo positivo, descartar las acciones que no hayan ayudado y generar nuevas instancias a partir de lo aprendido.

En caso de que la crisis digital se complemente con la difusión de noticias o informaciones falsas en canales analógicos se debe monitorear su alcance y darlas a conocer rápidamente a la Dirección General de Comunicación Estratégica del Viceministerio de Comunicación del MITIC.

MEDICIÓN Y MONITOREO DE REDES SOCIALES

MEDICIÓN Y MONITOREO EN REDES SOCIALES

MEDICIÓN DEL IMPACTO EN REDES

La principal ventaja de estar presente en estas plataformas es que entregan métricas en tiempo real sobre las interacciones que van teniendo cada una de las publicaciones realizadas. Esto permite obtener información sumamente útil, como por ejemplo testear diferentes temas en la opinión pública y comprobar su recepción y valoración. También se puede medir la cantidad de seguidores, alcance, visibilización y fidelidad de los contenidos publicados. De esta forma, se puede conocer el desempeño del Plan de Posteo implementado, y generar más contenido de aquel tipo que es mejor recibido.

Estos números se pueden obtener desde las mismas plataformas de publicación en redes sociales. No obstante, si los temas a evaluar adquieren grandes volúmenes de conversación, se recomienda considerar el uso de herramientas cuantitativas de terceros. Existen varias gratuitas como Hootsuite, HowSociable, Mention, SocialMention, GoogleAnalitics, etc.

Lo importante es identificar los datos que nos interesa incorporar al análisis de la evaluación de la red, para dar una mejor utilización a las métricas que nos brindan las plataformas.

CREACIÓN DE TÓPICOS PARA SU MONITOREO Y CLASIFICACIÓN. CONFIGURACIÓN DE PALABRAS CLAVE:

Las plataformas de medición pueden capturar sólo una muestra de todas las menciones que se realizan cada minuto en redes sociales.

El total es inmenso: muchas veces se trata de millones de comentarios, cada uno con sus características propias (idioma, geolocalización, privacidad, etc.). A raíz de esto, es vital que el Plan de Comunicación de la organización contenga temas de interés tanto para las publicaciones que se realicen desde sus propias cuentas, como para el monitoreo de la conversación general en redes sociales. Estos temas pueden derivar en palabras clave que pueden ser cargadas a la plataforma para su seguimiento.

Entonces, se debe identificar palabras clave que tengan que ver con la institución. Para MITIC por ejemplo las mismas podrían ser: tecnología, conectividad, ciberseguridad, Comunicación Estratégica, Campañas, redes sociales, etc. Luego se recomienda identificar hashtags que guarden relación con dichos temas. Estos datos nos permitirán saber de qué se está hablando en torno al tema que es de Interés Institucional, lo que nos podrá ayudar a tomar decisiones sobre si deberíamos subirnos o no a la conversación, si tenemos algo para aportar, o si deberíamos prepararnos para una posible crisis.

Como procedimiento, se recomienda que el encargado de redes sociales de la institución elija cinco palabras clave que tengan directa relación con la institución y la autoridad (el mismo nombre, por ejemplo). Otras palabras pueden surgir del análisis de las actividades que realiza la institución. Por ejemplo, la Secretaría de Emergencia Nacional (SEN) monitorea lo que guarda relación a los albergues mientras dure la emergencia sanitaria.

ANÁLISIS E INFORMES DE EVALUACIÓN DE LA RED SOCIAL:

Se recomienda realizar análisis semanales de la administración y movimientos de los perfiles de redes sociales. Los mismos deben incluir recomendaciones y conclusiones en base a las mediciones y al monitoreo realizado. Estos informes sirven para tomar decisiones estratégicas en tiempo real o de manera posterior, con el objetivo de mejorar la conversación con nuestra audiencia, aumentándola en cantidad y calidad.

MEDIDAS DE SEGURIDAD

MEDIDAS DE SEGURIDAD

Es responsabilidad de cada OEE velar por la implementación de buenas prácticas de seguridad o ciberhigiene en las cuentas oficiales institucionales y de cumplir con las directivas emitidas por el MITIC al respecto.

Siempre que la plataforma soporte múltiples cuentas de usuarios asignar las cuentas de usuarios autorizadas y aplicar los mismos controles de seguridad en las cuentas personales.

En caso que la herramienta no permita el uso o la gestión por múltiples cuentas, el Administrador deberá solicitar un protocolo de uso al Responsable de Seguridad de la Información (RSI) de la Institución que deberá realizar un análisis de riesgo y brindar las recomendaciones.

En caso de incidentes de seguridad en la cuenta, reportar el incidente de acuerdo a los lineamientos de las Resoluciones MITIC N° 432/2019 y N° 346/2020 y/o consultar inmediatamente las recomendaciones de la plataforma afectada y realizar los pasos indicados.

Es de suma importancia modificar cada cierto tiempo las contraseñas de acceso a las cuentas o perfiles de redes sociales, así como adoptar las nuevas medidas de seguridad.

RECOMENDACIONES PARA ESTABLECER CONTRASEÑAS SEGURAS:

- Utilizar al menos una letra en mayúscula
- Utilizar números
- Utilizar símbolos

Ejemplo: **#Contr@l0r1a**

La contraseña segura es fácil de recordar, debe seguir todas esas recomendaciones mencionadas y debe tener un sentido único para los gestores de las cuentas.

Se recomienda establecer una contraseña distinta para cada plataforma social, de modo que, si alguien ajeno a la institución descubre algún acceso, solamente podrá ingresar a una cuenta.

OPCIONES DE ROLES DE ADMINISTRADORES

No todas las redes sociales cuentan con una diversidad de roles de administradores. En tanto, Facebook si cuenta con una variedad de asignaciones desde:

- Administrador
- Editor
- Redactor, entre otros

En el caso particular de Facebook se recomienda asignar responsablemente a los/as administradores/as de la cuenta institucional, a fin de evitar inconvenientes en los roles y cumplimiento de actividades asignadas.

En caso de no poder acceder a alguna cuenta institucional acuda de inmediato al MITIC. Se sugiere además buscar información permanentemente en la página del CERT, ya que las plataformas de internet y redes sociales son muy dinámicas y están constante cambio.

OPCIONES DE PRIVACIDAD

La mayoría de las redes sociales tienen opciones personalizadas de privacidad. Se recomienda utilizarlas de forma adecuada, leyéndolas detenidamente y seleccionando la privacidad que mejor se adapta a la estrategia digital.

Es fundamental no suministrar información sensible: no utilizar datos personales del encargado de redes sociales al registrar cuentas (e-mails, claves, tarjetas de crédito).

Se recomienda el uso de un correo electrónico institucional, no vinculado a una persona específica, para registrar cuentas de plataformas gubernamentales, como, por ejemplo: *redessociales@mitic.gov.py*.

En caso de realizar pautas pagadas en redes sociales, se recomienda obtener una tarjeta de crédito pre-pago, a fin de evitar errores involuntarios. De esta manera, se podrá asignar el presupuesto a utilizar (en caso de contar con los recursos financieros), evitando gastos superiores.

AUTENTICACIÓN / VERIFICACIÓN EN DOS PASOS

Cada red social brinda un mecanismo que permite al usuario incluir un refuerzo en su seguridad al momento de acceder a sus cuentas, ya sea vía correo electrónico, WhatsApp, Facebook o Instagram.

Para habilitar la verificación en dos pasos se ingresa a: ***Ajustes/Configuración/Cuenta/Seguridad*** (dependiendo de cada red social) y aparece el texto *"Verificación en dos pasos"*.

ANEXOS

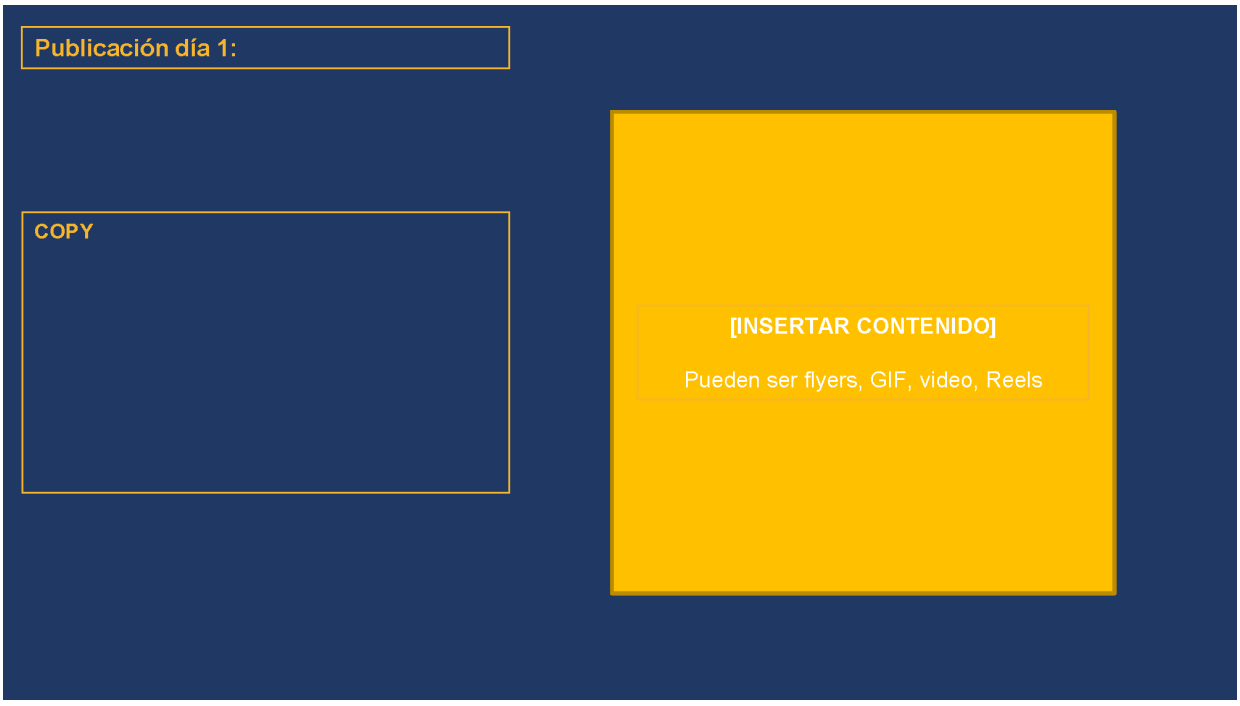
ANEXO 1

Plantilla del Plan de Posteos Semanales[2]

CALENDARIO DE POSTEOS

Días	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5
Lunes	*Ejemplo: Nuevo trámite en línea*				
Martes					
Miércoles					
Jueves					
Viernes					
Sábado					
Domingo					

En los espacios, insertar los temas de posteos para tener una visión general del mes



Publicación día 1:

COPY

[INSERTAR CONTENIDO]

Pueden ser flyers, GIF, video, Reels

[2]Descarga: *https://drive.google.com/drive/folders/1_wnZa7D5Zhgjsmb5PkrahH6IdoVn0xiG?usp=sharing*

ANEXO 2

FORMULARIO A[3]

ALTAS, BAJAS Y MODIFICACIONES (ABM) DE PERFILES CUENTAS OFICIALES INSTITUCIONALES EN PLATAFORMAS DIGITALES

1. ***Datos básicos del perfil:***
   Tipo de acción solicitada *(marcar con una X la opción seleccionada)*

ALTA	BAJA	MODIFICACIÓN	DESCRIPCIÓN

Completar los datos

Descripción de la cuenta:	
Nombre del perfil:	
Nombre del perfil: (alternativa)	
Cuenta de correo institucional asociada al perfil *(solo institucional)*	
Nombre de la Red Social:	
Objetivo:	
Otros datos:	

Autorización:

Firma y Sello de la MAI:	
Aclaración/C.I.:	
Fecha:	

[3]Descarga: *https://drive.google.com/drive/folders/1DIpTxZHMjDqLSdzr0JmuOZMyR-oifVYu?usp=share_link*

FORMULARIO B[4]

ALTAS, BAJAS Y MODIFICACIONES (ABM) DE USUARIOS DE CUENTAS OFICIALES INSTITUCIONALES EN PLATAFORMAS DIGITALES

1. ***Datos del personal autorizado a la acción solicitada (alta, baja o modificación)***
   Tipo de acción solicitada *(marcar con una X la opción seleccionada)*

ALTA	BAJA	MODIFICACIÓN	DESCRIPCIÓN

Completar los datos

Nombre y Apellido	
CI	
Dependencia	
Tipo vínculo *(nombrado, contratado, comisionado, pasante, etc.)*	
Institución de origen *(si aplica)*	
Correo electrónico institucional	
Celular	
Perfil y cuentas autorizadas	
Roles	
Otros datos:	

Obs:

Autorización:

Firma y Sello de la MAI:	
Aclaración/C.I.:	
Fecha:	

[4]Descarga: *https://drive.google.com/drive/folders/1DIpTxZHMjDqLSdzr0JmuOZMyR-oifVYu?usp=share_link*

ANEXO 3

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).
- 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 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.
- 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

ANEXO 4

Listado de herramientas complementarias

Acortado de URL: *https://app.bitly.com*

Calendario del Comunnity manager:
https://yiminshum.com/dias-fechas-festivos-paraguay-2020/
https://www.keysocialmediapy.com/descargarcalendario

Para programar publicaciones en diferentes plataformas:
https://play.google.com/store/apps/details?id=com.hootsuite.droid.full

Programar publicaciones en Instagram:
https://play.google.com/store/apps/details?id=com.apphi.android.post

Para compartir fotos de otra cuenta en Instagram:
https://play.google.com/store/apps/details?id=com.jaredco.regrann
https://play.google.com/store/apps/details?id=com.redcactus.repost

Para edición de videos
https://play.google.com/store/apps/details?id=com.wondershare.filmorago
https://play.google.com/store/apps/details?id=com.camerasideas.instashot&hl=es_419&gl=US

Para crear diseños:
https://play.google.com/store/apps/details?id=com.canva.editor
https://play.google.com/store/apps/details?id=com.delgeo.desygner

Guías de recomendaciones

- *Facebook:*
  https://es-la.facebook.com/gpa/best-practices/government-organization
- *Twitter:*
  https://business.twitter.com/es/basics/organic-best-practices.html
- *Instagram:*
  https://about.instagram.com/civic

Plataformas para analizar métricas

- *Creator Studio:*
  https://es-la.facebook.com/creators/tools/creator-studio
- *Metricool:*
  https://metricool.com/es/
- *Hootsuite:*
  https://www.hootsuite.com/es

Verificación en dos pasos

- *Twitter:*
  https://help.twitter.com/es/managing-your-account/two-factor-authentication
- *Facebook:*
  https://es-la.facebook.com/help/148233965247823
- *Instagram:*
  https://help.instagram.com/1582474155197965?locale=es_LA

Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

GOBIERNO
NACIONAL

Paraguay
de la gente