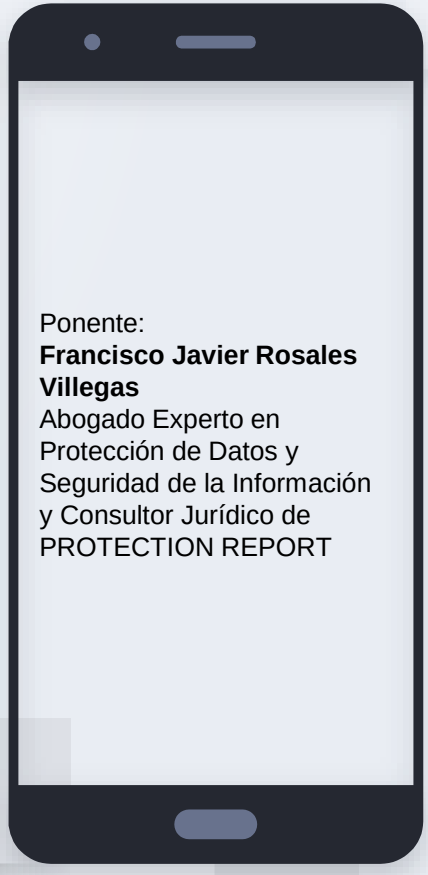
¿CÓMO PROTEJO LOS DATOS DE MI EMPRESA Y MI PRIVACIDAD?

PROTECTION REPORT®
PROTECCIÓN DE DATOS

“Si algo es GRATIS en INTERNET, el producto eres TU”



Ponente:
Francisco Javier Rosales Villegas
Abogado Experto en Protección de Datos y Seguridad de la Información y Consultor Jurídico de PROTECTION REPORT

PROTECTION REPORT®
PROTECCIÓN DE DATOS

¿QUIÉN ES PROTECTION REPORT?

CONSULTORA DE ÁMBITO NACIONAL, FUNDADA EN EL AÑO 2002, FORMADA POR MAS DE 25 PROFESIONALES Y ESPECIALIZADA EN PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN.

- **Alta especialización:** prestamos única y exclusivamente este tipo de servicios.
- **Amplia experiencia:** nos avala una trayectoria de más de 18 años, con más de 10.000 clientes de todos los sectores en toda España.
- **Atención personalizada y total disponibilidad y confianza:** nos adaptamos a su situación dándole una asistencia personalizada presencial permanente en sus instalaciones, para la solución de sus problemas de la manera más eficiente (le hacemos un traje a medida de sus necesidades).
- **Seguro de Responsabilidad Civil con la máxima cobertura por sanciones por la A.E.P.D.:** Que respalda la calidad de nuestro trabajo y responderá por cualquier defecto en nuestros servicios.
- **Garantía de cumplimiento de la Ley:** nuestros clientes cumplirán con las obligaciones exigidas por el Reglamento General de Protección de Datos 2016/679 y por la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.
- **Implantamos de forma directa** todos los procedimientos necesarios para cumplir con la Normativa en su empresa.
- **Precios competitivos** adaptados a sus necesidades, información y asesoramiento previo totalmente gratuitos.

PROTECTION REPORT®
PROTECCIÓN DE DATOS

¿POR QUÉ CUMPLIR CON ESTA NORMATIVA?

- La protección de la información y de los datos se ha convertido en una **obligación legal .**
- La información es **uno de los principales activos** que debe ser salvaguardado.
- **Legalidad de los tratamientos** de datos personales efectuados por la empresa.
- **Control de las actuaciones** que sus empleados lleven a cabo sobre la información.
- **Conocimiento de sus sistemas**, seguridad de los mismos y carencias y riesgos que presentan.
- **Adopción de medidas**, que ante sucesos le permitan continuar su actividad con el mínimo perjuicio posible.
- Que el personal conozca las tareas que le correspondan en materia de seguridad.

PROTECTION REPORT®
PROTECCIÓN DE DATOS

1.

EL DERECHO A LA PROTECCIÓN DE DATOS DURANTE LA CRISIS DEL CORONAVIRUS

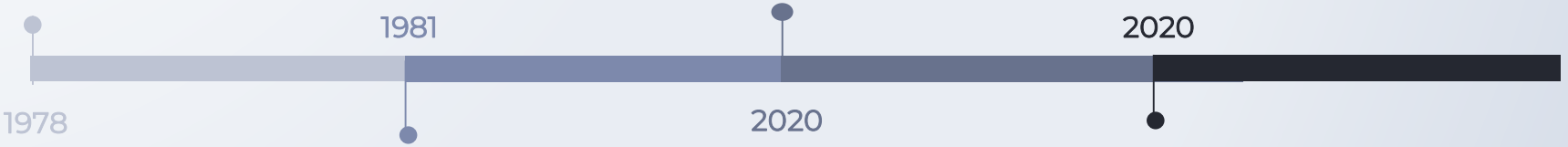
CRONOLOGÍA PRINCIPALES MEDIDAS LEGISLATIVAS

Constitución Española 8 (art. 116)

A través de Ley Orgánica se podrá regular los estados de alarma, de excepción y de sitio, y las competencias y limitaciones correspondientes.

Real Decreto 463/2020, de 14 de marzo

Por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el Covid-19.
Previsión de medidas dirigidas a proteger la salud y seguridad de los ciudadanos, contener la progresión de la enfermedad y reforzar el sistema de salud pública, además de prevenir y contener el virus y mitigar el impacto sanitario, social y económico.



Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio

Podrá ser decretado cuando se produzcan crisis sanitarias, como epidemias y situaciones de contaminación graves y permite limitar la circulación o permanencia de personas o vehículos en horas y lugares determinados, intervenir y ocupar transitoriamente industrias, fábricas, talleres o explotaciones de cualquier naturaleza, limitar o racionar el uso de servicios o el consumo de artículos de primera necesidad.

Real Decreto-Ley 8/2020, de 17 de marzo

De medidas urgentes extraordinarias para hacer frente al impacto económico y social del Covid-19.
También se han aprobado numerosas disposiciones por parte del Estado.

PROTECTION REPORT®
PROTECCIÓN DE DATOS

CONSENTIMIENTO Y BASES JURÍDICAS

Definición consentimiento:

Inequívoco
Libre
Revocable
Acto afirmativo claro, voluntario

Bases jurídicas de legitimación de un tratamiento de datos
Consentimiento expreso del interesado
Gestión de relación contractual entre las partes
Cumplimiento de una obligación legal
Interés legítimo
Protección de intereses vitales del interesado
Interés público

PROTECTION REPORT®
PROTECCIÓN DE DATOS

PRINCIPIOS DE PROTECCIÓN DE DATOS EN CUALQUIER TRATAMIENTO

- PRINCIPIO DE LICITUD, LEALTAD Y TRANSPARENCIA.
- PRINCIPIO DE LIMITACIÓN DE LA FINALIDAD: Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- PRINCIPIO DE MINIMIZACIÓN DE DATOS: Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- PRINCIPIO DE EXACTITUD: Exactos y, si fuera necesario, actualizados, exigiéndose al Responsable que adopte las medidas para que se rectifiquen o supriman los datos inexactos.
- PRINCIPIO DE LIMITACIÓN DEL PLAZO DE CONSERVACIÓN: Mantenidos durante no más tiempo del necesario.
- PRINCIPIO DE INTEGRIDAD Y CONFIDENCIALIDAD DE DATOS: Tratados de forma que se garantice una seguridad adecuada frente a intromisiones contra su pérdida o destrucción.

CUESTIONES A TENER EN CUENTA SOBRE EL CORONAVIRUS

A) ¿PUEDEN LOS EMPRESARIOS TRATAR LA INFORMACIÓN DE SI LAS PERSONAS TRABAJADORAS ESTÁN INFECTADAS DEL CORONAVIRUS?

B) ¿PUEDEN TRANSMITIR ESA INFORMACIÓN A OTRAS PERSONAS DE LA EMPRESA?

C) ¿SE PUEDEN TRATAR LOS DATOS DE SALUD DE LAS PERSONAS TRABAJADORAS RELACIONADOS CON EL COVID 19?

D) ¿EN CASO DE CUARENTENA PREVENTIVA O ESTAR AFECTADO POR EL CORONAVIRUS EL TRABAJADOR TIENE OBLIGACIÓN DE INFORMAR A SU EMPRESA DE ESTA CIRCUNSTANCIA?

E) ¿SE PUEDE PEDIR A LAS PERSONAS TRABAJADORAS Y VISITANTES AJENOS A LA EMPRESA DATOS SOBRE PAÍSES QUE HAYAN VISITADO ANTERIORMENTE, O SI PRESENTAN SINTOMATOLOGÍA RELACIONADA CON EL CORONAVIRUS?

F) ¿EL PERSONAL DE SEGURIDAD PUEDE TOMAR LA TEMPERATURA A LOS TRABAJADORES CON EL FIN DE DETECTAR CASOS CORONAVIRUS?

PROTECTION REPORT®
PROTECCIÓN DE DATOS

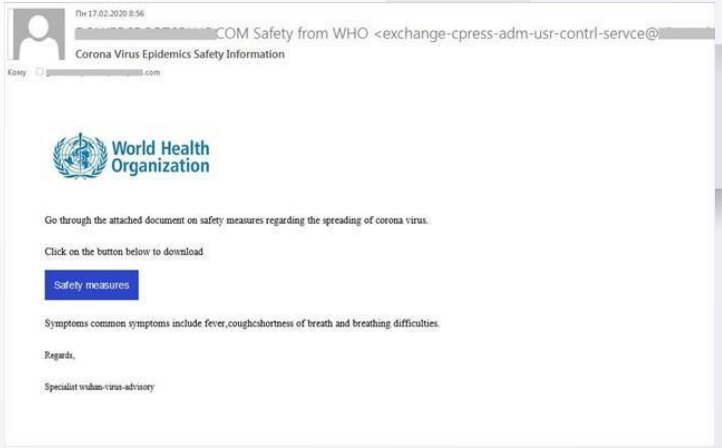
Control de temperatura

En esta zona se está realizando un control temporal de la temperatura corporal. Para poder acceder a la empresa es obligatorio realizar este control. El tratamiento de los datos obtenidos mediante este control se realizará de acuerdo con los siguientes detalles:

Responsable	Nombre de la empresa Calle Localidad
Finalidades	1. Proteger la salud y la vida de las personas que se encuentran en este centro de trabajo. 2. Contribuir a la contención de la pandemia. 3. Cumplir la normativa de prevención de riesgos laborales 4. Verificar el cumplimiento, por parte de los trabajadores, de la obligación de acudir al centro de trabajo sin fiebre.
Derechos	Puede ejercitar sus derechos de protección de datos enviado un mensaje de correo electrónico a la dirección xxx@empresa.com
Información completa	Puede acceder a la política de privacidad relativa a este tratamiento en www.empresa.es/privacidad-covid o solicitando un ejemplar en papel en la recepción de la empresa.

campus-ribas.com

CAMPAÑAS DE PHISHING SOBRE EL COVID-19



COM Safety from WHO <exchange-cpress-adm-usr-contrl-servce@

Corona Virus Epidemics Safety Information

World Health Organization

Go through the attached document on safety measures regarding the spreading of corona virus.

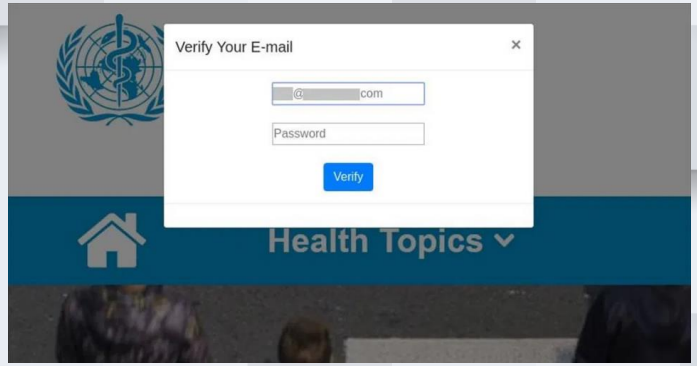
Click on the button below to download

Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Specialist wuhan-virus-advisory



MinSaludCol
@MinSaludCol

⚠️CUIDADO⚠️ Por e-mail y WhatsApp circula información falsa, a nombre del @MinSaludCol, que advierte la llegada del coronavirus a su sector, junto con un archivo que se instala en su dispositivo móvil y roba información personal. Informate solo en canales oficiales de MinSalud

Translate Tweet

From: Ministerio de Salud <comunicados@minsalud.gov.co>
Sent: Thursday, March 5, 2020 10:43:34 AM
Subject: Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted .

La salud es de todos Minsalud

Estimado ciudadano

Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación

Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos aislado los sitios en los cuales no le recomendamos visitar ya que estos se encuentran a pocos metros de su residencia

Adjuntamos un archivo pdf este se encuentra con una clave es : salud

FALSO

GDT Guardia Civil
@GDTGuardiaCivil

#NiCaso a este mensaje que circula por #Whatsapp. Suplantan al Ministerio de Sanidad @sanidadgob para dar supuestas "recomendaciones" contra el #coronavirus #COVID19 y un enlace para venderte mascarillas.

Translate Tweet

+34 632 en línea

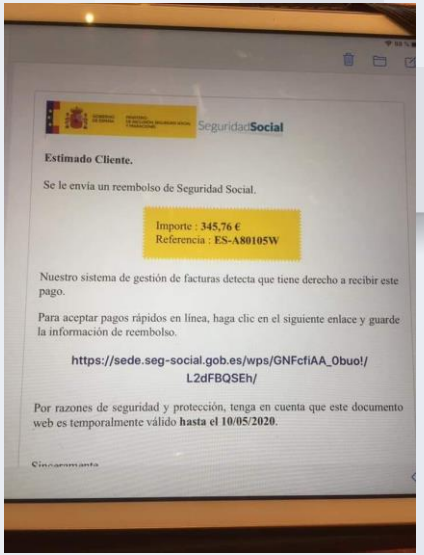
ALERTA POR CORONAVIRUS
Mensaje **urgente** del Ministerio de Sanidad:

http://www. coronavirus.es

Reenvíos a la población ciudadana y máxima difusión de este mensaje ¡Compártelo en tus grupos de WhatsApp y en tus Redes Sociales! **¡¡PUEDES SALVAR VIDAS!!**

Es muy importante que siga las medidas de protección recomendadas:

#NiCaso



SeguridadSocial

Estimado Cliente.

Se le envía un reembolso de Seguridad Social.

Importe : **345,76 €**
Referencia : **ES-A80105W**

Nuestro sistema de gestión de facturas detecta que tiene derecho a recibir este pago.

Para aceptar pagos rápidos en línea, haga clic en el siguiente enlace y guarde la información de reembolso.

https://sede.seg-social.gob.es/wps/GNFcfiAA_0buo!/ L2dFBQSEh/

Por razones de seguridad y protección, tenga en cuenta que este documento web es temporalmente válido **hasta el 10/05/2020**.

Sinceramente

PROTECTION REPORT®
PROTECCIÓN DE DATOS

RECOMENDACIONES PARA EVITAR EL PHISHING

Infórmate mediante fuentes oficiales y confiables, acude directamente a las webs de las instituciones, nunca a través de un enlace en un mensaje o en un email.

Fíjate bien en el contenido del mensaje, sospecha de mensajes con faltas de ortografía, errores gramaticales y saludos genéricos sin aportar ningún dato tuyo como “Estimado ciudadano” o “Estimado paciente”

Verifica la dirección de email remitente del mensaje y también el enlace web al que te remite el mensaje, a veces los enlaces se parecen mucho a las direcciones legítimas.

Sospecha mucho más si además el contenido del mensaje te urge a realizar cualquier tipo de acción cuanto antes, con una urgencia injustificada.

Cuidado con las solicitudes de datos personales a través de webs a las que has llegado siguiendo un enlace contenido en un mensaje o correo electrónico. Mejor accede directamente a la web de esa organización.

Ante una situación de riesgo lo más importante es guardar la tranquilidad y reflexionar antes de actuar o tomar decisiones precipitadas.

PROTECTION REPORT®
PROTECCIÓN DE DATOS

AEPD WEBS Y APPS QUE OFRECEN AUTOEVALUACIONES Y CONSEJOS SOBRE EL CORONAVIRUS

La Agencia Española de Protección de Datos (AEPD) ha constatado que están proliferando páginas web y aplicaciones móviles que ofrecen ayuda y servicios para autoevaluar y aconsejar en relación con el Coronavirus.
La AEPD quiere advertir al conjunto de la ciudadanía de los riesgos que implica el facilitar categorías de datos sensibles, como son los relativos a la salud, a estas webs y apps, incluso en aquellos casos en los que aparentemente esos datos no se asocian a la identidad del usuario que utiliza la aplicación.
La Agencia ha podido constatar que algunas páginas web y apps no aportan la detallada información exigible para identificar a los responsables, ni incluyen las finalidades para las que podrían tratarse los datos, incluso se han detectado casos en los que se suplanta al Ministerio de Sanidad.
La Agencia va a iniciar actuaciones de investigación para constatar estos tratamientos ilícitos de datos personales, identificar a sus responsables e imponerles en tal caso importantes sanciones económicas.

PROTECTION REPORT®
PROTECCIÓN DE DATOS

2.

LA PROTECCIÓN DE DATOS EN SITUACIONES DE MOVILIDAD Y TELETRABAJO

A) POLÍTICA PROTECCIÓN DE INFORMACIÓN EN SITUACIONES DE MOVILIDAD

- Necesidades concretas y los riesgos por el acceso a recursos corporativos desde espacios que no están bajo el control de la organización.
- Formas de acceso remoto permitidas, tipo de dispositivos válidos y el nivel de acceso permitido en función de los perfiles de movilidad definidos.
- Responsabilidades y obligaciones que asumen los empleados, suministrando guías funcionales para su formación.
- Información de las principales amenazas por las que pueden verse afectados y las posibles consecuencias de incumplir esas directrices.
- Comunicación de cualquier incidente que afecte a datos personales.
- Recomendable firmar un acuerdo de teletrabajo que incluya los compromisos adquiridos en esa situación de movilidad.

B) ELEGIR SOLUCIONES Y PROVEEDORES DE SERVICIOS CON GARANTÍAS

- No utilizar aplicaciones y soluciones de teletrabajo que no ofrezcan garantías y que puedan dar lugar a la exposición de los datos personales.
- Recurrir a proveedores que ofrezcan soluciones probadas y garantías suficientes que eviten la exposición de los datos personales.
- Si estos proveedores acceden a datos personales, tendrán la consideración de encargados de tratamiento y se debe regular dicha relación.

C) RESTRINGIR EL ACCESO A LA INFORMACIÓN

- Los perfiles o niveles de acceso a los recursos y a la información tienen que configurarse en función de las funciones de cada empleado.
- Aplicar restricciones de acceso adicionales en función del tipo de dispositivo desde el que se acceda

D) CONFIGURAR PERIÓDICAMENTE LOS EQUIPOS Y DISPOSITIVOS

- Los servidores de acceso remoto han de ser revisados y asegurarse que están correctamente actualizados y configurados.
- Los equipos corporativos utilizados tienen que:

Estar actualizados a nivel de aplicación y sistema operativo.

Tener deshabilitados los servicios que no sean necesarios.

Configuración por defecto de mínimos privilegios.

Instalar aplicaciones autorizadas.

Software antivirus y cortafuegos actualizados.

Activar solo comunicaciones wifi, bluetooth, NFC… y puertos USB u otros necesarios para llevar a cabo las tareas.

Mecanismos de cifrado de la información.

Comunicación de cualquier incidente que afecte a los datos.

- Si se usan dispositivos personales de los empleados, restringir la conexión a una red segregada con acceso limitado a aquellos recursos que se hayan identificado como menos críticos y sometidos a menor nivel de riesgo.

PROTECTION REPORT®
PROTECCIÓN DE DATOS

E) MONITORIZAR LOS ACCESOS A LA RED CORPORATIVA DESDE EL EXTERIOR

- Sistemas de monitorización para identificar patrones anormales de comportamiento en el tráfico de red para evitar la propagación de malware.
- Comunicación de las brechas de seguridad que afecten a datos personales a la Autoridad de Control y/o a los interesados.
- Informar al personal para estas situaciones de movilidad, sobre la existencia y el alcance de estas actividades de control y supervisión.
- Si las actividades de monitorización se usaran para verificar el cumplimiento de las obligaciones laborales se debería informar previamente a tal efecto.
- Estos mecanismos de monitorización deben respetar los derechos digitales establecidos en la LOPDGDD.
- La configuración para el acceso remoto debe revisarse periódicamente.

F) GESTIONAR RACIONALMENTE LA PROTECCIÓN DE DATOS Y LA SEGURIDAD

- Análisis de riesgos para evaluar la proporcionalidad entre los beneficios a obtener de ese acceso a distancia y el impacto potencial de ver comprometido el acceso a la información de personal.
- La política debe contener los procedimientos para auditar los dispositivos de acceso remoto, los procedimientos de administración y monitorización y los servicios proporcionados por proveedores y la forma en que la política es actualizada a los riesgos existentes.
- Valoración del riesgo que represente la pérdida de un recurso y la exposición o acceso no autorizado a la información manejada.
- Planificar y evaluar la aplicaciones de acceso cumpliendo con los principios de privacidad desde el diseño y por defecto en todas sus etapas.

¿CÓMO DEBE ACTUAR EL EMPLEADO EN ESTAS SITUACIONES?

- Respetar la política de protección de la información en situaciones de movilidad.
- Proteger el dispositivo utilizado en movilidad y el acceso al mismo:

  • Contraseñas de acceso robustas.

  • No instalar aplicaciones no autorizadas.

  • No conectarse a la red desde lugares públicos.

  • Mantener los mecanismos de autenticación.

  • No utilizar el equipo corporativo con fines particulares y si es personal evitar simultanear las dos actividades.

  • Antivirus actualizado.

  • Verificar la legitimidad de los correos electrónicos recibidos.

  • Desactivar las conexiones WIFI, bluetooth y similares que no estén utilizadas…

- Garantizar la protección de la información que se está manejando:
  - Evitar la entrada y salida de documentación en soporte papel y destruirla correctamente.
  - Extremar las precauciones para evitar el acceso no autorizado a la información personal.
  - Prevenir que se puedan escuchar conversaciones por parte de terceros ajenos.
- Guardar la información en los espacios de red habilitados:
  - No de forma local en el dispositivo, sino utilizando recursos compartidos o en la nube.
  - Si se usan equipos personales no utilizar aplicaciones no autorizadas.
  - No bloquear la política de copia de seguridad corporativa del dispositivo.
  - Revisar y eliminar periódicamente la información residual del dispositivo.
- Si la información se ha visto comprometida comunicar con carácter inmediato la brecha de seguridad.

.

3.

¿WHATSAPP O TELEGRAM? ¿QUÉ APLICACIÓN ES MÁS SEGURA?

PROTECTION REPORT®
PROTECCIÓN DE DATOS

COMPARATIVA APLICACIONES

	WHATSAPP	TELEGRAM
Año creación	2009	2013
N° de usuarios	2.000 millones	200 millones
Arquitectura	Conexión vía servidores, un único dispositivo	Basado en la nube, permite varios dispositivos
Plataforma	Android, iOS, BlackBerry, Nokia, Web, Windows, Mac	Android, iOS, Firefox OS, Web, Windows, Mac, Linux
Cifrado	Extremo a extremo basado en Signal, usado en todas las comunicaciones	MTProto, extremo a extremo sólo en chat secretos, servidor-cliente en el resto

WHATSAPP:
- LIMITACIÓN REENVÍO MENSAJES
- CENSURA
- SISTEMA DE VERIFICACIÓN DE CONTENIDOS

PROTECTION REPORT®
PROTECCIÓN DE DATOS

COMPARATIVA APLICACIONES

	WHATSAPP	TELEGRAM
Envíos	Fotos, vídeo, música, ubicación, contactos, documentos de cualquier tipo, clips de voz	Fotos, vídeo, música, ubicación, clips de voz, clips de vídeo, contactos, encuestas (en grupos) y cualquier archivo de hasta 1,5 GB
Chats de grupo	Hasta 256 personas	Hasta 200.000 miembros
Bots	Aún no de forma generalizada	Sí
Stickers	Sí	Sí
Videollamadas	Sí, hasta cuatro personas	No

COMPARATIVA APLICACIONES

	WHATSAPP	TELEGRAM
Llamadas	Sí	Sí
Widgets	Sí	No, solo en accesos a conversaciones
Temas	Solo normal u oscuro	Sí, muy personalizable
Añadir contactos	Automáticamente desde los contactos del teléfono	Posibilidad de añadir nombre de usuario
Uso de almacenamiento	Se puede liberar espacio desde la propia App	Se puede limitar el espacio máximo de la caché desde la propia aplicación
Copia de seguridad	En Google Drive	No es necesaria, está cifrada en la nube

4.

SEGURIDAD EN VIDEOLLAMADAS O VIDEOCONFERENCIAS

PROTECTION REPORT®
PROTECCIÓN DE DATOS

¿ES SEGURA LA APLICACIÓN ZOOM?

PROTECTION REPORT®
PROTECCIÓN DE DATOS

GRACIAS!

Alguna pregunta?

De todas formas pueden contactar en:

- 902364585 / 958294383
- jrosales@protectionreport.com

www.protectionreport.com

PROTECTION REPORT®
PROTECCIÓN DE DATOS