

Nº Expediente: 00001-00087215

Fecha entrada: 19 de enero de 2024

Interesado/a: [REDACTED]

En la fecha indicada, tuvo entrada en la Unidad de Información y Transparencia del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, la solicitud de acceso a la información pública de la referencia, al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG).

Con fecha de 19 de enero de 2024, esa solicitud fue recibida en el Gabinete del Ministro de Asuntos Exteriores, Unión Europea y Cooperación. A partir de esa fecha, comienza el cómputo de plazo de un mes, previsto en el artículo 20.1 de la Ley 19/2013, para su resolución.

Analizada la solicitud el Gabinete del Ministro de Asuntos Exteriores, Unión Europea y Cooperación

RESUELVE:

Conceder acceso parcial a la información y señala que:

Los teléfonos móviles a disposición de empleados públicos son proporcionados y configurados por la Administración General del Estado. Para garantizar su seguridad y correcto uso, la Secretaría General de Administración Digital (SGAD), junto con la colaboración del Centro Criptológico Nacional (CCN), gestiona la seguridad de los dispositivos móviles de las entidades de la AGE que están dentro del alcance del Contrato Centralizado de Comunicaciones.

De forma adicional, existe un servicio integral, gestionado por Presidencia del Gobierno, de la movilidad corporativa y la seguridad de los dispositivos entregados en el Marco General de Funcionamiento del Servicio de Comunicaciones y Dispositivos móviles para ciertos cargos del Gobierno y de la Administración General del Estado. Los usuarios del servicio especial de comunicaciones y dispositivos móviles son los miembros del Consejo de Ministros y de la Comisión de Secretarios de Estado y Subsecretarios.

Existen, además, mecanismos de protección y seguridad en los dispositivos móviles entre los que destacamos los siguientes:

- Solución EMM (Del inglés Enterprise Mobility Management) para la administración, monitorización y control de la configuración de los dispositivos móviles corporativos
- Herramienta MTD (Del Inglés Mobile Threat Defense), que es una solución proactiva de defensa frente a amenazas móviles.

- Android Enterprise (AE), que proporciona protecciones de seguridad básica, políticas de administración y funciones de red.

El protocolo señala que las aplicaciones requeridas para realizar actividades de comunicación se deben instalar en los dispositivos exclusivamente para uso de marketing público e información, y no vinculados a cuentas personales. Para garantizar un uso correcto y seguro de estos dispositivos, la AGE hace auditorias o comprobaciones sobre el uso de los dispositivos corporativos y la instalación de aplicaciones. Todas las herramientas que componen los servicios a disposición de los empleados públicos son imprescindibles para garantizar el cumplimiento legal de protección de datos de carácter personal, en base al Reglamento General de Protección de Datos (GDPR), así como la protección de la información corporativa acorde con las medidas de seguridad requeridas por el Esquema Nacional de Seguridad (ENS) o cualquier otra normativa legal que, por la naturaleza del servicio, se le pudiera aplicar.

Por último, cabe señalar que la Administración General del Estado está en constante desarrollo de diversas medidas de carácter técnico para garantizar la seguridad y un uso adecuado de las redes sociales en los dispositivos utilizados.

Por lo que respecta al cargo que ocupan las personas que usan la aplicación, el modelo de dispositivo, el dominio de correo electrónico, la red, las versiones de sistema operativo y el número de dispositivos, se consideran datos susceptibles, especialmente por su naturaleza técnica, de ser explotados para la realización de ciberataques, por lo que no se pueden suministrar por razones de salvaguarda de seguridad. El éxito de un ciberataque a alguno de los dispositivos a que se hace referencia podría entrañar una amenaza para toda la red y, por lo tanto, para la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública o los intereses económicos, siendo por lo tanto de aplicación las excepciones del artículo 14.1. en sus letras a), b), c), d) y h) de Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Se recuerda que, de conformidad con lo señalado en el artículo 15.5 de la Ley 19/2013, el tratamiento posterior que se pudiera hacer de los datos personales obtenidos a través del presente ejercicio del derecho de acceso a la información pública se encuentra sometido a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD); de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, así como demás normativa vigente sobre protección de datos personales.

Contra la presente Resolución, que pone fin a la vía administrativa, podrá interponerse recurso contencioso-administrativo ante el órgano judicial competente (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa),

en el plazo de dos meses o, previa y potestativamente, reclamación ante el Consejo de Transparencia y Buen Gobierno, en el plazo de un mes. En ambos casos, el plazo se contará desde el día siguiente al de notificación de la presente Resolución. Ello, sin perjuicio de cualquier otro recurso o reclamación que se estime procedente.

(firmado electrónicamente)

El Director del Gabinete del Ministro de Asuntos Exteriores, Unión Europea y
Cooperación

Sergio Cuesta Francisco