Defensa blinda su red informática para evitar un 'caso Wikileaks'

El ministerio podrá "monitorizar e inspeccionar" el uso de correos electrónicos

Miguel González Madrid

ELPAIS.COM 5-08-2012

Soldados españoles destacados en Irak, en la base de Diwaniya en marzo de 2004. / Joseph Barrak (AFP)

El Ministerio de Defensa ha blindado sus sistemas de información y telecomunicaciones para prevenir ataques, atajar abusos y evitar la repetición en España de un *caso Wikileaks*, la filtración de cientos de miles de documentos clasificados que sufrieron en 2010 el Pentágono y el Departamento de Estado de EE UU. Los más de 50.000 usuarios de la denominada Red de Propósito General del Ministerio de Defensa (WAN PG) —que conecta al órgano central, el Estado Mayor de la Defensa, los tres ejércitos y las unidades desplegadas en el exterior, entre otros centros y organismos— deben firmar el denominado Formulario de Conformidad, por el que aceptan las normas del código de uso de la misma y se comprometen a cumplirlas.

Dicho código, aprobado en abril pasado, encomienda al Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa (Cosdef) las "labores de monitorización continua, registro e inspección de los sistemas de información y telecomunicaciones, que permitan detectar de una forma temprana los posibles incidentes de seguridad y, en caso de materializarse, emprender las acciones reactivas pertinentes que minimicen su impacto y conlleven a su resolución". El control afecta a todos los

servicios proporcionados a través de la WAN PG, incluyendo comunicaciones, acceso a bases de datos, correo electrónico o navegación por Internet.

El código, elaborado por la Subdirección General de Tecnologías de la Información y Comunicaciones, proclama su intención de garantizar "la preservación de los derechos fundamentales de las personas reconocidos en la Constitución española", como la intimidad, el secreto de las comunicaciones y la protección de datos de carácter personal, pero se reserva la facultad de monitorizar e inspeccionar el empleo de la red por parte de los usuarios; ya sean militares, empleados civiles del Ministerio de Defensa o personal de empresas contratadas.

Los 50.000 usuarios del sistema deben firmar que aceptan ser controlados

El propio código aclara que entiende por *monitorizar* la posibilidad de "observar, mediante los medios técnicos apropiados, el uso que se hace de los sistemas de información y telecomunicaciones .. e identificar los intentos de comprometer su seguridad, con el objetivo de proteger dichos sistemas y la información que estos manejan". Respecto a la facultad de *inspeccionar*, la define como la posibilidad de "examinar los registros de actividad de cualquier sistema de información y telecomunicaciones ... para garantizar el cumplimiento de los requisitos de seguridad correspondientes".


USO OFICIAL

Anexo I. FORMULARIO DE CONFORMIDAD DEL USUARIO

USO OFICIAL

FORMULARIO DE CONFORMIDAD CON EL CÓDIGO DE USO DE LOS SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES QUE UTILIZAN LA INFRAESTRUCTURA TECNOLÓGICA DE LA RED DE PROPÓSITO GENERAL DEL MINISTERIO DE DEFENSA

NOMBRE:

APELLIDOS:

UCO/EMPRESA:

CARGO:

Reconozco haber leído y entendido el documento de "Código de uso de los Sistemas de Información y Telecomunicaciones que utilizan infraestructura tecnológica de la Red de Propósito General del Ministerio de Defensa", y acepto los términos y condiciones de uso establecidos en el mismo, estando de acuerdo en cumplirlos, y en atender a las modificaciones al documento que me hayan sido debidamente comunicados.

_____ a ____ de _____ de _____

El usuario

USO OFICIAL

USO OFICIAL

Ningún usuario podrá alegar que el control de sus comunicaciones supone una invasión de su intimidad, pues el código determina que la infraestructura y los equipos del ministerio "únicamente son para fines oficiales, no pudiendo ser utilizados con carácter privado", y califica de "abuso" cualquier uso "que trascienda los fines estrictamente laborales o profesionales".

Además, se “registrará la información del uso que los usuarios hacen de los sistemas de información y telecomunicaciones y se archivará dicha información, de modo que se asegure su integridad y se impida su pérdida accidental o alteración”. No explica durante cuánto tiempo se almacenará esta información ni cómo podrán los afectados conocerla y pedir su cancelación o modificación.

Entre las infracciones que incluye el código figuran las de “manejar información clasificada en sistemas que no estén autorizados para ello”; “manejar información relacionada con actividades ilegales, así como contenidos pornográficos o denigrantes que puedan herir la moral o la dignidad de las personas ... o dañar la imagen de las Fuerzas Armadas”; “copiar o extraer datos de carácter personal”; o “efectuar cualquier actividad de carácter comercial o lucrativo”. Además, se castigará a quienes traten de “eludir los sistemas de seguridad y control”; descarguen o instalen un programa sin autorización; conecten sin permiso un equipo portátil que no sea del ministerio; cedan las credenciales a un tercero para que pueda acceder a la red o realicen cualquier actividad que pueda congestionarla o degradarla.

Todos los usuarios deberán denunciar “de manera inmediata cualquier sospecha en cuanto a una mala utilización de dichos sistemas u otro tipo de incidencia que pueda afectar a la seguridad de la información”.

El código advierte de que el incumplimiento de sus normas, sea intencionado o negligente, podrá suponer la limitación total o parcial del acceso a la red por parte del infractor, “sin perjuicio de las acciones legales que pudieran derivarse”.

Además, “dependiendo de la excepcionalidad de la situación”, Defensa podrá retirar la autorización de acceso a la red antes de que esta decisión sea comunicada al propio afectado.