ÚLTIMA HORA 26/03/2020 19:43

El CCN-CERT fomenta la formación en ciberseguridad con un nuevo curso online sobre principios y recomendaciones básicas (/comunicacion-eventos/comunicados-ccn-cert/9772-nuevo-curso-online-sobre-principios-y-recomendaciones-basicas-en-ciberseguridad-para-toda-la-ciudadania.html)

CCN-CERT AV 14/20 Respuesta a las consultas sobre la renovación de certificados

Detalles
Publicado: 26 Marzo 2020

AVISOS

Respuesta a las consultas sobre la renovación de certificados

Fecha de publicación: **26/03/2020**

Durante el estado de alarma, decretado por la pandemia del COVID-19, el **acceso a los servicios de la Administración General del Estado** por vía telemática adquiere una especial relevancia para mantener en funcionamiento los servicios del Estado.

El Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional, **CCN-CERT**, ha recibido diversas consultas relacionadas con la renovación de los certificados electrónicos para la gestión de trámites de forma segura con la Administración Pública y Entidades Privadas a través de Internet.

En este sentido, se recuerda que es posible renovar telemáticamente (sin personación física) los certificados expedidos por la Fábrica Nacional de Moneda y Timbre (FNMT-RCM) a ciudadanos y representantes únicos o solidarios, durante los 60 días anteriores a la fecha de extinción del periodo de vigencia de dichos certificados.

Hasta ahora, en cumplimiento de la normativa legal aplicable, solo se permitía realizar una única renovación, siendo necesaria la personación en una oficina de registro para acreditar la identidad si se quería obtener un nuevo certificado.

No obstante, y de acuerdo con el 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, la **FNMT-RCM está trabajando para permitir la renovación de estos tipos de certificados sin tener en cuenta si hubo una renovación anterior**. Por tanto, se podrá solicitar la renovación de este tipo de certificados de forma telemática, identificándose con un certificado activo que está próximo a caducar, evitando así la necesidad de acudir a una oficina de registro.

Se espera que en los próximos días, la FNMT-RCM anuncie en su sede electrónica (www.sede.fnmt.gob.es (https://www.sede.fnmt.gob.es/)) esta posibilidad.

Todo ello, no exime a las administraciones de continuar trabajando a corto plazo, y solo como medida excepcional, en la **implementación de medidas técnicas alternativas y temporales** para permitir el acceso a sus sistemas hasta que la problemática asociada a la renovación de los Certificados sea subsanada.

Para más información, puede consultar la información publicada por la FNMT-RCM a través de su página, www.fnmt.es (http://www.fnmt.es/).

Atentamente,

Equipo CCN-CERT

//

El CCN-CERT (www.ccn-cert.cni.es (https://www.ccn-cert.cni.es/)) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es (https://www.ccn.cni.es/)), adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

Claves PGP Públicas
---
info@ccn-cert.cni.es (mailto:info@ccn-cert.cni.es) / ccn-cert@ccn-cert.cni.es (mailto:ccn-cert@ccn-cert.cni.es)

Fingerprint: 2933 AE1E CB92 548D 6515 B11B 88E9 B0C3 F9CC 1235
Descarga (https://www.ccn-cert.cni.es/documentos-publicos/1354-public-ccn-cert-global/file.html)

//

POLÍTICA DE PRIVACIDAD:
El 25 de mayo de 2018 entró en vigor el Reglamento de Protección de Datos (RGPD) de la Unión Europea (UE). Dicho Reglamento está diseñado para unificar los requisitos de privacidad de los datos en toda la UE. Desde el **Centro Criptológico Nacional** siempre hemos prestado la mayor atención y realizado todos los esfuerzos necesarios para mantener la privacidad de nuestros usuarios y suscriptores y, por supuesto, cumplir con la Normativa vigente. Con el objetivo de adecuarnos al RGPD hemos actualizado nuestra política de privacidad para ampliar lo que veníamos haciendo hasta la fecha: otorgar a su información personal el respeto y la seguridad que se merece.

Nos pondremos en contacto con usted cuando dispongamos de información que consideremos que le pueda ser de interés, informándole de contenidos, servicios, eventos, avisos de seguridad o, si procede, gestionar y atender sus solicitudes de información.

Puede encontrar la nueva información y política de privacidad del **Centro Criptológico Nacional** haciendo click AQUÍ (https://www.ccn-cert.cni.es/politica-de-privacidad.html). Por favor, consulte esta información y no dude en ponerse en contacto con nosotros para cualquier aclaración enviándonos un email a info@ccn-cert.cni.es (mailto:info@ccn-cert.cni.es)

//

AVISO DE CONFIDENCIALIDAD:
El presente mensaje va dirigido de manera exclusiva a su destinatario.
Si usted no es el destinatario de este mensaje (o la persona responsable de su entrega), considérese advertido de que lo ha recibido por error, así como de la prohibición legal de realizar cualquier tipo de uso, difusión, reenvío, impresión o copia del mismo. Si ha recibido este mensaje por error, por favor notifíquelo al remitente y proceda a destruirlo inmediatamente.

© 2020 Centro Criptológico Nacional, Argentona 30, 28023 MADRID

Anterior (/seguridad-al-dia/avisos-ccn-cert/9763-ccn-cert-av-15-20-vulnerabilidades-en-google-chrome.html)

Siguiente (/seguridad-al-dia/avisos-ccn-cert/9739-ccn-cert-av-13-20-sesion-de-vanesa-sobre-seguridad-en-sistemas-de-correo-electronico.html)

Volver (/)

Mapa web

(http://www.defensa.gob.es/) (http://www.cni.es/) (https://www.ccn.cni.es/)

(http://www.cert.org/csirts/cert_authorized.html) (http://www.first.org/)

(https://www.trusted-introducer.org/) (http://www.egc-group.org/)

(https://ec.europa.eu/inea/en/connecting-europe-facility) (https://www.csirt.es/)