# USTIC-INFO 02/22. Últimos Documentos de Seguridad CCN-STIC del CCN-CERT publicados

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, informa de que el **CCN-CERT**, del Centro Criptológico Nacional**, ha publicado durante los últimos seis meses** una serie de **documentos de seguridad**, denominados Series CCN-STIC, entre los que se incluyen guías, informes de buenas prácticas o *abstracts*, que son **de interés para vuestro conocimiento y aplicación, en aquellos sistemas de vuestra competencia.**

## Documentos CCN-STIC

Las Series CCN-STIC **son normas, instrucciones, guías y recomendaciones** desarrolladas por el Centro Criptológico Nacional **con el fin de mejorar el grado de ciberseguridad de las organizaciones**. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

El grueso de las Series está especialmente **dirigidas al personal de las Administraciones Públicas** y empresas y organizaciones de interés estratégico (parte privada del portal) y otras de difusión pública para todos los usuarios.

### *Últimas Guías de Seguridad Publicadas*

A continuación, en la siguiente tabla, se presentan las guías de seguridad publicadas en los últimos seis meses, indicando una breve descripción, la fecha de publicación y un enlace a las mismas para su consulta:

| Guía | Descripción | Publicación | Archivo/Enlace |
|---|---|---|---|
| CCN-STIC-620 Guía de aplicaciones de perfilado de seguridad para Oracle Linux | • El objetivo es aportar los procedimientos adecuados para aplicar un perfilado de seguridad basado en la realización de un análisis de riesgos en sistemas que implementen Oracle Linux 8.<br>• Este documento incluye una descripción de uso de esta guía, una declaración de riesgos, la identificación de valor de riesgo y, por último, un perfilado de seguridad en el que se establecen las medidas de seguridad a aplicar. | Agosto 2022 | CCN-STIC 620 Perfilado de Seguridad Oracle Linux.pdf |

| | | | |
|---|---|---|---|
| CCN-STIC-573A21 Implementación de seguridad en servidor de ficheros sobre Microsoft Windows Server 2019 | • El fin de este documento es el de aplicar un perfilado de seguridad en base a un análisis de riesgos preceptivo, en sistemas que implementan servidores Windows Server 2019 y que actúen como servidor de ficheros.<br>• Incluye una descripción de uso de esta guía, una declaración de riesgos, la identificación de valor de riesgo y, por último, un perfilado de seguridad en el que se establecen las medidas de seguridad a aplicar al producto o tecnología tratado en la presente guía.<br>• Junto a la guía, se encuentra su correspondiente script para su correcta implementación. | Julio 2022 | CCN-STIC 573A21 Servidor de Ficheros en WS2019.pdf<br><br>*Scripts*:<br><br>CCN-STIC 573A21 Servidor de Ficheros en WS2019 - Scripts.zip |
| CCN-STIC-1615 Procedimiento de empleo seguro SUSE Linux Enterprise Server 15 SP2 | • Esta guía reúne las consideraciones necesarias para configurar de manera segura SUSE Linux Enterprise Server (SLES) 15 SP2. | Junio 2022 | CCN-STIC 1615 PES SUSE 15 SP2.pdf |
| CCN-STIC-1432 Procedimiento de empleo seguro ARUBA OS-CX | • Se proporcionan las directrices de seguridad y mejores prácticas para las características y protocolos de gestión proporcionados por el software ARUBA OS-CS versión 10.06.<br>• Pone el foco en las funcionalidades que pueden ser relevantes para una configuración segura del equipo para evitar que sea un vector de ataque. | Junio 2022 | CCN-STIC-1432 PES Aruba OS-CX.pdf |
| CCN-STIC-1434 Procedimiento de empleo seguro Sonicwall SMA | • El objeto de esta guía es facilitar la instalación y configuración segura de los dispositivos de Sonicwall Secure Mobile Access (SMA) con la versión de software 12.1, junto con el aseguramiento del entorno en el que se despliega. | Mayo 2022 | CCN-STIC-1434 PES Sonicwall SMA.pdf |
| CCN-STIC-1612 Procedimiento de empleo seguro F5 BIG-IP LTM+APM | • Recoge el procedimiento de empleo seguro para el sistema F5 BIG-IP LTM+APM versión 14.1.0.3 con la revisión HotfixBIGIP-14.1.0.3.0.75.6-ENG. | Mayo 2022 | CCN-STIC-1612 PES F5 BIG-IP LTM+APM.pdf |
| | | | |

| | | | |
|---|---|---|---|
| Guías CCN-STIC 889C, 889D, 889E y 889F de configuración segura para Oracle OCI – Arquitecturas Híbridas, OCI Database – Instancias VM, OCI Compute – Instancias VM y Bare Metal y C@C Sistemas Exadata - Autonomous DB. | • Son cuatro guías de configuración segura de los servicios de Oracle Cloud Infraestructure (OCI) y de Oracle Cloud at Customer (O-C@C).<br>• El documento CCN-STIC 889C, muestra el despliegue y configuración de los servicios Oracle OCI, identificando los servicios para las Arquitecturas Híbridas en entornos de cliente-nube para aquellas organizaciones que necesiten conectar sus centros de datos a la nube de Oracle, cumpliendo con las medidas de seguridad del ENS.<br>• Por su parte, la CCN-STIC 889D pretende servir de guía para la configuración de los servicios de Base de datos de Oracle Cloud Infrastructure (OCI) para cargas de trabajo en la nube pública de Oracle. La utilidad principal es identificar los servicios e instancias de bases de datos en máquinas virtuales que deban configurarse.<br>• La tercera guía CCN-STIC 889E muestra el despliegue y configuración de OCI para cargas de trabajo en la nube pública, identificando los servicios de cómputo para las Instancias de máquina virtual (MV) y bare metal.<br>• El cuarto documento, la guía CCN-STIC 889F, muestra la configuración de los servicios de Oracle Cloud at Customer (O-C@C) para cargas de trabajo en la nube privada de Oracle, identificando los servicios de C@C Sistemas Exadata y Autonomous DB. | Abril 2022 | • CCN-STIC-889C CS Oracle OCI-Arquitecturas Híbridas.pdf |

| | | | |
|---|---|---|---|
| | | | • CCN-STIC-889D_CS Oracle OCI Database - Instancias VM.pdf<br>• CCN-STIC-889E_CS Oracle OCI Compute - Instancias VM y Bare Metal.pdf<br>• CCN-STIC-889F CS Oracle C@C Sistemas Exadata-Autonomous DB. pdf |

## *Últimos Informes de Buenas Prácticas y Abstracts Publicados*

Además de las anteriores guías comentadas, hay que destacar otros documentos de seguridad CCN-STIC de interés. Se trata de dos informes de buenas prácticas y un *abstract*, tal como puede apreciarse en la siguiente tabla, donde se indica una breve explicación, fecha de publicación y enlace para su lectura:

| Documento | Descripción | Publicación | Archivo/Enlace |
|---|---|---|---|
| CCN-STIC BP/26 Recomendaciones de seguridad en Microsoft Edge | • El propósito de este documento consiste en establecer los procedimientos y utilidades necesarias para implementar y garantizar la seguridad en Microsoft Edge, frente a los riesgos a los que este pueda estar expuesto.<br>• Se proporciona una serie de pasos e instrucciones que permitan la configuración adecuada del navegador de forma manual. Así mismo se proporciona un archivo de configuración para aplicar medidas de seguridad y así facilitar la posibilidad de implementar seguridad. | Agosto 2022 | CCN-CERT_BP-26 Recomendaciones de seguridad en Microsoft Edge.pdf |
| CCN-STIC BP/22 Recomendaciones de seguridad para Oracle Database 19C | • Este documento establece los procedimientos y utilidades necesarias para implementar y garantizar la seguridad para Oracle Database 19C<br>• Es importante tener en cuenta los aspectos de seguridad que se configuran en el ámbito del sistema operativo, como usuarios, servicios, comunicaciones y protocolos. En el caso de Oracle 19C, el proceso de verificación de identidad de usuario se realiza fuera del entorno de la aplicación como LDAP, OS, TNS, Kerberos, por SID o nombre de servicio. | Junio 2022 | CCN-CERT_BP22-Recomendaciones de seguridad para Oracle Database 19C.pdf |
| *Abstract* "Lecciones aprendidas de seguridad para la prestación de servicios electrónicos" | • Documento con las lecciones aprendidas y recomendaciones de seguridad sobre la prestación de servicios electrónicos.<br>• La seguridad a la hora de implementar y desplegar este tipo de servicios se ha convertido en un factor determinante. El aumento de su demanda ha provocado que se conviertan en el punto de mira de los atacantes y afianzar su seguridad a través de lecciones aprendidas y recomendaciones ayudará a reducir el número de ciberataques. | Junio 2022 | Abstract - Seguridad en Servicios Electronicos.pdf |

Para cualquier duda o consulta al respecto, podéis contactar con nuestro equipo en ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

**Unidad de Seguridad TIC**

**Subdirección de Tecnologías de la Información y Comunicaciones**

**Servicio Andaluz de Salud**