centro criptológico nacional

Perfil de Cumplimiento Especifico
CCN-STIC 886

Perfil de Cumplimiento Especifico para LORETO-NG
(Solución de Cloud Privado o Comunitario)

Noviembre 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.12.07 23:29:11 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-304-9

Fecha de Edición: noviembre de 2022

ÍNDICE

1. INTRODUCCIÓN

1. En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.
2. Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 311/2022, de 3 de mayo, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.
3. Las Guías CCN-STIC, del Centro Criptológico Nacional, podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de requisitos, medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.
4. El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, como se dispone en el artículo 30.3 del ENS, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible, todo ello de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.
5. Las auditorías se realizarán en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en el Anexo I y Anexo III del Real Decreto 311/2022, de 3 de mayo, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.
6. A tal fin, tras realizar un análisis de riesgos contemplando las vulnerabilidades y amenazas a las que hace frente el uso de esta tecnología en las entidades del Sector Público, y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando el siguiente **Perfil de Cumplimiento Especifico para garantizar la seguridad en la solución de Cloud privado o comunitario LORETO-NG Base, basada en Nextcloud.**

2. TECNOLOGÍAS IMPLICADAS

7. El presente Perfil de Cumplimiento Específico podrá ser de aplicación a los sistemas de información de aquellas organizaciones que, tras el correspondiente proceso de categorización, precise de unas **necesidades de seguridad hasta categoría ALTA,** sin perjuicio de la aplicación de otras disposiciones normativas que emanen del Esquema Nacional de Seguridad o de cualesquiera otras regulaciones que resulten asimismo de aplicación, tales como la normativa en materia de Protección de Datos, por ejemplo.
8. La tecnología empleada en LORETO-NG se basa en Nextcloud, una solución se código abierto para crear servicios de alojamiento de archivos, haciéndolo sobre servidores Red Hat Enterprise Linux 9, empleando diferentes contenedores *Docker* y *Docker-compose* como orquestador.
9. De acuerdo con lo establecido en la Guía de seguridad de las TIC *CCN-STIC-823 Utilización de servicios en la Nube*, las nubes con modelos de despliegue **privados** son aquellas que se basan en una infraestructura operada únicamente por una organización y que ofrecen servicios únicamente a esa misma organización.
10. Por su parte, las nubes con modelos de despliegue **comunitarios** se definen como aquellas alojadas en infraestructuras compartidas por varias organizaciones, relacionadas entre ellas compartiendo requisitos de servicio, donde uno de los miembros del colectivo controla la infraestructura.
11. El presente Perfil de Cumplimiento Específico podrá ser de aplicación, bajo las premisas previamente dispuestas, tanto en los sistemas alojados en infraestructuras propias de la entidad interesada, como alojados en infraestructuras contratadas a proveedores de servicios de alojamiento físico en centros de datos (*housing - colocation*), siempre y cuando la responsabilidad de administración y configuración segura de la plataforma recaigan sobre la propia organización que contrata.

3. DECLARACIÓN DE APLICABILIDAD

12. Como es sabido, la declaración de aplicabilidad comprende el conjunto de medidas de seguridad que son de aplicación para el cumplimiento del ENS en un sistema de información concreto. Tal conjunto de medidas dependerá de la categoría del sistema y de los niveles asociados a las dimensiones de seguridad.
13. En el Anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se tiene en cuenta para cada medida de seguridad, no únicamente la aplicabilidad de requisitos base, sino la de posibles refuerzos obligatorios.
14. Se ha determinado así, para la solución de Nube privada o comunitaria basada en LORETO-NG Base, las medidas que son de aplicación, y, en caso de aplicar, la exigencia de los diferentes requisitos base y de los posibles refuerzos obligatorios,

mediante una tabla modulada mediante los comentarios del apartado 4 de este mismo documento.

15. En la tabla de criterios de aplicación se reproduce literalmente la exigencia de requisitos base y refuerzos obligatorios del Anexo II del ENS, únicamente para nivel/categoría Alto/Alta, al ser la considerada para este perfil de cumplimiento específico para LORETO-NG. No obstante, en la columna 'Nota' de la derecha se referencian los criterios de aplicación que pueden contener la matización o la exclusión de algún refuerzo.

Medidas de Seguridad		Dimensiones de seguridad afectadas	Nivel de las dimensiones de seguridad ALTO Categoría del Sistema ALTA	Nota
org	**Marco organizativo**			
org.1	Política de seguridad	Todas	aplica	
org.2	Normativa de seguridad	Todas	aplica	4.1
org.3	Procedimientos de seguridad	Todas	aplica	
org.4	Proceso de autorización	Todas	aplica	
op	**Marco operacional**			
op.pl	Planificación			
op.pl.1	Análisis de riesgos	Todas	+ R2	
op.pl.2	Arquitectura de Seguridad	Todas	+ R1 + R2 + R3	4.2
op.pl.3	Adquisición de nuevos componentes	Todas	aplica	
op.pl.4	Dimensionamiento/gestión de la capacidad	D	+ R1	
op.pl.5	Componentes certificados	Todas	aplica	4.3
op.acc	Control de acceso			4.4
op.acc.1	Identificación	T A	+ R1	
op.acc.2	Requisitos de acceso	C I T A	+ R1	
op.acc.3	Segregación de funciones y tareas	C I T A	+ R1	
op.acc.4	Protección de gestión de derechos de acceso	C I T A	aplica	
op.acc.5	Mecanismo autenticación (usuarios externos)	C I T A	+ [R2 o R3 o R4] + R5	4.5
op.acc.6	Mecanismo autenticación (usuarios organización)	C I T A	+ [R1oR2oR3oR4] +R5+R6+R7+R8+R9	4.6
op.exp	Explotación			
op.exp.1	Inventario de activos	Todas	aplica	
op.exp.2	Configuración de seguridad	Todas	+ R1	4.7
op.exp.3	Gestión de la configuración de seguridad	Todas	+ R1 + R2 + R3	
op.exp.4	Mantenimiento y actualizaciones de seguridad	Todas	+ R1 + R2	4.8
op.exp.5	Gestión de cambios	Todas	+ R1	
op.exp.6	Protección frente a código dañino	Todas	+ R1 + R2 + R3 + R4	
op.exp.7	Gestión de incidentes	Todas	+ R1 + R2 + R3	
op.exp.8	Registro de la actividad	Todas	+ R1 + R2 + R3 + R4 + R5	4.10
op.exp.9	Registro de la gestión de incidentes	Todas	aplica	
op.exp.10	Protección de claves criptográficas	Todas	+ R1	4.11
op.ext	Recursos externos			

op.ext.1	Contratación y acuerdos de nivel de servicio	Todas	aplica	
op.ext.2	Gestión diaria	Todas	aplica	
op.ext.3	Protección de la cadena de suministro	Todas	aplica	
op.ext.4	Interconexión de sistemas	Todas	+ R1	
op.nub	Servicio en la nube			
op.nub.1	Protección de servicios en la nube	Todas	+ R1 + R2	4.12
op.cont	Continuidad del servicio			4.13
op.cont.1	Análisis de impacto	D	aplica	
op.cont.2	Plan de continuidad	D	aplica	
op.cont.3	Pruebas periódicas	D	aplica	
op.cont.4	Medios alternativos	D	aplica	4.14
op.mon	Monitorización del sistema			
op.mon.1	Detección de intrusión	Todas	+ R1 + R2	
op.mon.2	Sistema de métricas	Todas	+ R1 + R2	
op.mon.3	Vigilancia	Todas	+ R1 + R2 + R3 + R4 + R5 +R6	
mp	**Medidas de protección**			
mp.if	Protección de las instalaciones e infraestructuras			4.15
mp.if.1	Áreas separadas y con control de acceso	Todas	aplica	
mp.if.2	Identificación de las personas	Todas	aplica	
mp.if.3	Acondicionamiento de los locales	Todas	aplica	
mp.if.4	Energía eléctrica	D	+ R1	
mp.if.5	Protección frente a incendios	D	aplica	
mp.if.6	Protección frente a inundaciones	D	aplica	
mp.if.7	Registro de entrada y salida de equipamiento	Todas	aplica	
mp.per	Gestión del personal			
mp.per.1	Caracterización del puesto de trabajo	Todas	aplica	
mp.per.2	Deberes y obligaciones	Todas	+ R1	
mp.per.3	Concienciación	Todas	aplica	
mp.per.4	Formación	Todas	aplica	
mp.eq	Protección de los equipos			
mp.eq.1	Puesto de trabajo despejado	Todas	+ R1	
mp.eq.2	Bloqueo de puesto de trabajo	A	+ R1	4.16
mp.eq.3	Protección de dispositivos portátiles	Todas	+ R1 + R2	
mp.eq.4	Otros dispositivos conectados a la red	C	+ R1	
mp.com	Protección de las comunicaciones			
mp.com.1	Perímetro seguro	Todas	aplica	4.17
mp.com.2	Protección de la confidencialidad	C	+ R1 + R2 + R3	4.18
mp.com.3	Protección de la integridad y autenticidad	I A	+ R1 + R2 + R3 + R4	4.18
mp.com.4	Separación de flujos de información en la red	Todas	+ [R2 o R3] + R4	4.19
mp.si.	Protección de los soportes de información			4.20
mp.si.1	Marcado de soportes	C	aplica	n/a
mp.si.2	Criptografía	C I	+ R1 + R2	n/a
mp.si.3	Custodia	Todas	aplica	n/a

mp.si.4	Transporte	Todas	aplica	n/a
mp.si.5	Borrado y destrucción	C	+ R1	4.21
mp.sw	Protección de las aplicaciones informáticas			
mp.sw.1	Desarrollo de aplicaciones	Todas	+ R1 + R2 + R3 + R4	4.22
mp.sw.2	Aceptación y puesta en servicio	Todas	+ R1	4.23
mp.info	Protección de la información			
mp.info.1	Datos personales	Todas	aplica	4.24
mp.info.2	Calificación de la información	C	aplica	4.25
mp.info.3	Firma electrónica	I A	+ R1 + R2 + R3 + R4	4.11
mp.info.4	Sellos de tiempo	T	aplica	n/a
mp.info.5	Limpieza de documentos	C	aplica	4.26
mp.info.6	Copias de seguridad	D	+ R1 + R2	4.27
mp.s	Protección de los servicios			
mp.s.1	Protección del correo electrónico	Todas	aplica	4.28
mp.s.2	Protección de servicios y aplicaciones web	Todas	+ R2 + R3	
mp.s.3	Protección de la navegación web	Todas	+ R1	n/a
mp.s.4	Protección frente a denegación de servicio	D	+ R1	4.29

Detalles del criterio de aplicación de la medida en el apartado 4 de este documento.

Se considera que la medida, salvo excepciones, no será de aplicación a LORETO-NG.

3.1 MEDIDAS DE APLICACIÓN

16. Aplican al presente Perfil de Cumplimiento Específico para LORETO-NG **65 de las 73 medidas de seguridad** definidas en el citado Anexo II del RD 311/2022 para sistemas de categoría ALTA.

17. Algunas medidas de seguridad no se proporcionan con LORETO-NG, debiendo ser implementadas por la organización donde se implanta dicha solución, o bien aprovechar las ya disponibles, incorporando LORETO-NG a su ámbito de protección.

18. Asimismo, otras medidas se considera que no aplican a este tipo de soluciones, al igual que en otras se ha modificado o eliminado algún refuerzo obligatorio, al considerarse que no es necesario para este perfil de cumplimiento específico. Dichas medidas se resumen a continuación:

Marco Operacional:

[op.pl.5] Componentes certificados

[op.exp.6] Protección frente a código dañino

[op.nub.1] Protección de servicios en la nube

Medidas de Protección:

[mp.si.1] Marcado de soportes

[mp.si.2]	Criptografía
[mp.si.3]	Custodia
[mp.si.4]	Transporte
[mp.sw.1]	Desarrollo de aplicaciones
[mp.info.4]	Sellos de tiempo
[mp.s.3]	Protección de la navegación web

4. CRITERIOS DE APLICACIÓN DE MEDIDAS

4.1 [ORG.2] Normativa de seguridad

19. La organización donde se implante LORETO-NG puede disponer de diferentes documentos independientes de normativa interna, o bien disponer de varios de ellos consolidados en un documento de "*uso de medios electrónicos puestos por la organización a disposición de sus empleados y colaboradores*". En cualquier caso, debería actualizarse dicha normativa contemplando el uso correcto e indebido de LORETO-NG.

4.2 [OP.PL.2] Arquitectura de seguridad

20. El modelo de despliegue de la solución LORETO-NG es de Cloud privada o comunitaria, lo que implica deba ser instalada en modo local (*on-premise* o *in-house*), por lo que se requiere que el proveedor de la solución aporte el/los correspondiente(s) diagramas de arquitectura, según se determina en el apartado 5.1 *Presentación y arquitectura de la solución*, de la Guía CCN-STIC 858 *Implantación de sistemas SaaS en modo local (on-premise)*.

4.3 [OP.PL.5] Componentes certificados

21. El equipamiento hardware que se emplee para soportar la solución LORETO-NG que corre sobre Red Hat Enterprise Linux 9, debe estar certificado, incluyendo los componentes de seguridad que formen parte de la infraestructura en la que se integra.
22. Si no es posible que dichos componentes o los elementos software estén certificados, entonces se deberán aplicar **medidas complementarias de vigilancia**, según se determinan en el apartado 4.4 de la Guía CCN-STIC 808 *Verificación del cumplimiento del ENS*.
23. Un ejemplo de medida complementarias de vigilancia sería que, tras acordar el Comité de Seguridad la renovación de dichos componentes por otros certificados cuando sea posible (por ejemplo a su renovación), aumentar la monitorización sobre los mismos, prestando atención a los anuncios de vulnerabilidades de seguridad (CVE) por parte del fabricante y del CERT de referencia, entre otros

orígenes, al tiempo que se instalan diligentemente los consecuentes parches correctivos de seguridad que solucionen las referidas vulnerabilidades.

4.4 [OP.ACC] Mecanismos de Autenticación (en general)

24. Puesto que la solución LORETO-NG se basa en Nextcloud, es posible la creación, modificación o supresión de usuarios locales, así como la sincronización de éstos mediante LDAP, Keycloak, Directorio Activo, o con otros servicios estándar de administración de accesos e identidades (IAM).
25. Si la gestión de usuarios se apoya en una sincronización externa, dicha gestión deberá cumplir con las disposiciones del ENS referidas a [op.acc] *Control de acceso*.
26. En el caso de configurar Nextcloud con su propia validación local de usuarios y contraseñas, debe verificarse si es necesario actualizar o completar, por ejemplo, la "*Política de acceso lógico*" o el "*Procedimiento de gestión de usuarios*" en base a la referida gestión local.
27. Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por LORETO-NG no puedan ser aplicados -como en el caso de los equipos de usuario empleados para la administración del sistema-, serán de aplicación las medidas que determine la organización en base al RD 311/2022 en la categoría y nivel ALTO.

4.5 [OP.ACC.5] Mecanismo de autenticación (usuarios externos)

28. Nextcloud permite activar la autenticación de doble factor (2FA) de manera nativa, en base a mecanismos OTP, como son las Apps tipo 'Google Authenticator' o 'Microsoft Authenticator' instaladas en el *smartphone* del usuario. En cambio, LORETO-NG no emplea de forma nativa certificados como mecanismo de autenticación, requiriéndose en este caso soluciones adicionales.
29. El administrador del sistema LORETO-NG, partiendo de los *logs* generados, podría llegar a elaborar un script para auditar qué usuarios no han activado el 2FA y actuar en consecuencia, o bien, siendo la opción recomendable, forzar a los grupos de usuarios a configurar obligatoriamente dicho 2FA en su primer acceso.

4.6 [OP.ACC.6] Mecanismo de autenticación (usuarios de la organización)

30. En el caso de querer emplear validación mediante certificados, será necesario integrar LORETO-NG con un servicio de gestión de identidades (IAM) que permita el uso de sistemas de validación con certificado como, por ejemplo, *Cl@ve*.
31. LORETO-NG, aún configurado de forma local, dispone de su propia gestión de *logs* donde se recogen todas las trazas, incluidos los accesos de usuario, pudiéndose enviar éstas a un agregador de *logs* o a un SIEM.

4.7 [OP.EXP.2] Configuración de Seguridad

32. Para la configuración de LORETO-NG se han tenido en cuenta las guías CCN-STIC que se relacionan a continuación, que deberán seguir aplicándose durante todo el ciclo de vida de la solución, atendiendo a la aparición de nuevas versiones:
    - Guía CCN-STIC 826 Implementación de Seguridad Nextcloud + Guía CCN-STIC 826 ANEXO A.
    - Guía CCN-STIC 858 Implantación de sistemas SaaS en modo local (*on-premise*).
    - Guía CCN-STIC 888C Configuración segura para Contenedores.
    - Guía CCN-STIC 610A22: Aplicación De Perfilado De Seguridad Para Red Hat Enterprise Linux.
    - Guía CCN-STIC 652A Seguridad en Contenedores.
    - Guía CCN-STIC 667 Contenerización en Arquitecturas Virtuales + Guía CCN-STIC 667 ANEXO B.
33. El resto de componentes del sistema deberán tener una configuración de seguridad asociada, siguiendo los requisitos exigidos en el Anexo II del ENS y en base a guías CCN-STIC, o de cualquier otro origen incluyendo al fabricante.

4.8 [OP.EXP.4] Mantenimiento y actualizaciones de seguridad

34. La solución LORETO-NG, por sí sola, no dispone de un proceso automático de verificación de nuevas versiones o parches de seguridad de todos sus elementos.
35. No obstante, Red Hat sí que realiza dicha verificación sobre sus componentes, de forma nativa si se configura al efecto, pudiendo establecerse el envío de un correo electrónico al administrador.
36. Será responsabilidad del administrador de la solución verificar las actualizaciones y parches disponibles para todos los componentes, en base a un procedimiento al efecto.

4.9 [OP.EXP.6] Protección frente a código dañino

37. La solución LORETO-NG incluye su propio antivirus basado en *ClamAV*, que consiste en un software antimalware de código abierto (con licencia GPL) para GNU/Linux.
38. Las trazas, avisos y alertas generadas por *ClamAV* deben enviarse al SIEM para su integración en la gestión centralizada de *logs* de la organización.
39. *ClamAV* no dispone de la capacidad de implementar listas blancas. No obstante, al estar orientado al entorno cerrado de LORETO-NG, se excluye el refuerzo obligatorio [op.exp.6.r3] para categoría ALTA en éste perfil de cumplimiento.

40. En relación al también refuerzo obligatorio para categoría ALTA [op.exp.6.r4] se deberá dotar de soluciones EDR a los '*endpoints*' o equipos de usuario de la organización que acceden a LORETO-NG, como a cualquier otro recurso.

4.10 [OP.EXP.8] Registro de Actividad de los Usuarios

41. La solución LORETO-NG configurada de forma local y aislada del Directorio Activo, o equivalente, dispone de un sistema de *logs* propio donde recoge todas las trazas que genera.
42. Será responsabilidad de la organización donde se implante dicha solución en modo local enviar los *logs* a un agregador o, directamente, al SIEM de la organización.
43. Asimismo, será responsabilidad de la organización proveer los mecanismos necesarios para asegurar los registros de actividad de la solución LORETO-NG, el acceso no autorizado a los mismos y su preservación mediante copias de seguridad.

4.11 [OP.EXP.10] Protección de Claves criptográficas y [MP.INFO.3] Firma electrónica

44. La solución LORETO-NG requiere un certificado de servidor para cifrar las comunicaciones de acceso mediante, por ejemplo, el protocolo TLS.
45. Contratar un certificado a un Prestador de Servicios de Confianza Cualificado y aportarlo a la solución es responsabilidad de la organización donde se implanta LORETO-NG.
46. Como decimos, dicho certificado digital de servidor deberá ser cualificado, y haber sido expedido por un Prestador de Servicios de Confianza Cualificado, inscrito en la "*Lista de confianza de prestadores cualificados de servicios electrónicos de confianza (TSL)*":

    https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

    o según la "*Trusted List Browser*" de la Comisión Europea, según establece el Reglamento Europeo eIDAS:

    https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home
47. En cualquier caso, la organización donde se implante LORETO-NG debe proteger el certificado durante las fases de su ciclo de vida que estén bajo su responsabilidad, entre las siguientes: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

4.12 [OP.NUB.1] Protección de servicios en la Nube

48. Esta medida no será de aplicación implícita, dado que LORETO-NG se implanta en modo local (*on-premise*) proporcionando soluciones de Cloud privado o comunitario.

49. Otra cuestión es que la organización donde se implante complemente LORETO-NG con algún servicio Cloud público, en cuyo caso se aplicaría esta medida únicamente a dichos servicios complementarios.

4.13 [OP.CONT] Continuidad del servicio

50. Cuando se haya valorado la dimensión de disponibilidad como de nivel ALTO, debe garantizarse la continuidad de los servicios soportados mediante la solución LORETO-NG.
51. En ese caso, deben incorporarse al Análisis de Impacto en el Negocio (BIA) los servicios prestados por LORETO-NG.
52. De la misma manera, la solución LORETO-NG debe considerarse dentro del Plan de Continuidad de la organización en la que se implante, incluyendo la realización de pruebas del mismo.

4.14 [OP.CONT.4] Medios alternativos

53. La infraestructura asociada a LORETO-NG, basada en *Dockers*, permite realizar un Plan de Continuidad y de Recuperación relativamente simple, con tiempos cortos, pudiendo replicarse la configuración entre infraestructuras ubicadas en varios emplazamientos.
54. No obstante, dotar al sistema de medios alternativos será responsabilidad de la organización donde se implante la solución LORETO-NG y dependerá de la infraestructura y recursos comunes disponibles.
55. Se pueden implantar soluciones de hiperconvergencia (HCI) entre diferentes *datacenters*, que se apoyan en un hipervisor, almacenamiento definido por software y redes virtualizadas, consiguiendo alta disponibilidad.
56. También son posibles soluciones más simples, aunque menos efectivas, como un mecanismo que permita la realización de copias de seguridad de LORETO-NG con la periodicidad necesaria para poder cumplir con los criterios de disponibilidad de los servicios acorde a la guía CCN-STIC 803 *Valoración de los Sistemas*[1].

4.15 [MP.IF] Protección de las instalaciones e infraestructuras

57. Al tratarse LORETO-NG de una solución de Cloud privado o comunitario, que se implanta en modo local (*on-premise*) en la infraestructura de la organización, se considerará aplicable este grupo de medidas en categoría ALTA, moduladas algunas de ellas en función del nivel de la dimensión Disponibilidad.

[1] Se establecen en cuatro (4) horas de RTO para sistemas de nivel ALTO en la dimensión de disponibilidad. Una posible materialización sería efectuar un volcado de la base de datos de Nextcloud seguida de un *snapshot* del referido volcado y de los ficheros almacenados.

4.16 [MP.EQ.2] Bloqueo del puesto de trabajo

58. La solución LORETO-NG permite definir la cancelación de las sesiones establecidas una vez transcurrido determinado intervalo de las mismas sin detectarse actividad.
59. No obstante, el administrador de la organización donde se implante la solución deberá, en función del uso de la misma en lo que se refiere a tamaño de los archivos que los usuarios puedan llegar a almacenar y del ancho de banda disponible para cada transferencia, definir el período de cancelación de sesiones lo suficientemente holgado para permitir que las subidas de archivos, especialmente las remotas, puedan concluir.

4.17 [MP.COM.1] Perímetro seguro

60. La protección del perímetro es responsabilidad de la organización donde se implante LORETO-NG, dado que dicha protección suele ser común para toda la red.
61. No obstante, LORETO-NG únicamente requiere mantener abierto el puerto 443 (estándar para HTTPS), salvo que se le adicionen otros posibles elementos, siempre a criterio de la organización.

4.18 [MP.COM.2] Protección de la confidencialidad y [MP.COM.3] Protección de la integridad y la autenticidad

62. Si la solución LORETO-NG da servicio a usuarios de la organización, éstos podrán materializar los accesos protegiéndolos mediante VPNs disponibles en la propia organización, que se recuerda deben estar basadas en doble factor de autenticación (2FA) para accesos atravesando zonas no seguras, como es internet.
63. Para los usuarios externos a la organización donde se implanta LORETO-NG, la protección se basará en el protocolo empleado, por ejemplo, TLS para conseguir un tráfico cifrado HTTPS.

4.19 [MP.COM.4] Separación de flujos de información en la red

64. Con independencia de la separación de flujos que deba realizar la organización en su red interna para cumplir con los requisitos del ENS para esta medida, la solución LORETO-NG está basada en contenedores, lo que le permite mantenerse de forma aislada en la misma máquina.

4.20 [MP.SI] Protección de los soportes de información

65. Este grupo de medidas, a excepción de [mp.si.5] *Borrado y destrucción,* aplica únicamente a soportes removibles tipo pendrives, discos USB, DVDs y otros de naturaleza análoga, por lo que no se consideran en el ámbito de la solución LORETO-NG.

66. Cuestión distinta es si el personal de administración de dicha solución en la organización requiere su uso, en cuyo caso se atenderá a las disposiciones del ENS.

4.21 [MP.SI.5] Borrado y destrucción

67. Al tratarse LORETO-NG de una solución de Cloud privado o comunitario, implantada sobre la infraestructura de la organización, al final del ciclo de vida de sus componentes de almacenamiento deberán ser estos destruidos o aplicárseles técnicas de borrado seguro con alguna solución certificada, como puede ser la herramienta OLVIDO del CCN.

4.22 [MP.SW.1] Desarrollo de Aplicaciones

68. Esta medida no será de aplicación, dado que los componentes de la solución ya están desarrollados externamente. Al emplearse componentes de código abierto, el proceso de puesta en marcha consiste únicamente en la integración y parametrización de los mismos.
69. No obstante, todos los contenedores de LORETO-NG, al ser creados, son chequeados con una herramienta que los analiza respecto a la base de datos de CVE para asegurar que no contienen vulnerabilidades conocidas en el código.
70. Por otra parte, no deben realizarse otras tareas de desarrollo en el mismo entorno de producción que soporta la solución LORETO-NG, como se supone dispone la normativa interna de la organización.

4.23 [MP.SW.2] Aceptación y puesta en servicio

71. Es responsabilidad de la organización donde se implante la solución LORETO-NG realizar, previamente a su puesta en producción, un *pentesting* o auditoría técnica para detectar posibles vulnerabilidades de seguridad asociadas a la integración de LORETO-NG con el sistema preexistente de la organización.
72. Por otro lado, acompañan a la solución al menos las tres (3) guías o manuales que determina la Guía CCN-STIC 858 Implantación de sistemas SaaS en modo local (*on-premise*), consistentes en una "*guía de instalación y configuración segura del sistema*", dirigida a administradores, una "*guía de uso seguro del sistema*", dirigida a usuarios de la solución, y una "*guía de relación entre cliente y proveedor*", donde se determina qué es responsabilidad de cada parte (el proveedor de la solución y la organización donde se implanta).
73. Todo ello, con independencia de que se aporten otros manuales complementarios que se consideren de utilidad.

4.24 [MP.INFO.1] Datos personales

74. Es responsabilidad de la organización donde se implanta la solución LORETO-NG, previamente a su puesta en producción, realizar preceptivo análisis de riesgos para los derechos y libertades de los titulares de los datos personales exigido en

el RGPD, así como verificar si resulta necesario o no realizar una Evaluación de Impacto en la Protección de Datos (EIPD).

75. Del mismo modo, deben considerarse otros aspectos que determina el RGPD o la LOPDGDD, considerando que para el sector público las medidas de seguridad necesarias para proteger datos de carácter personal, según la Disposición adicional primera de la LO 3/2018 (LOPDGDD), serán las del ENS.

4.25 [MP.INFO.2] Calificación de la Información

76. Esta medida será de aplicación a todos aquellos documentos que formen parte del sistema de gestión de la seguridad de la información relacionados con la solución LORETO-NG (normas internas, procedimientos, instrucciones técnicas, manuales, etc.) y a los relativos al funcionamiento y normas de uso de los servicios que se pongan a disposición de los usuarios apoyados en la solución.
77. No será exigible la aplicación de esta medida en los documentos compartidos por los usuarios haciendo uso de los servicios Cloud de LORETO-NG.

4.26 [MP.INFO.5] Limpieza de documentos

78. Esta medida será de aplicación en todos aquellos documentos que formen parte del sistema de gestión de la seguridad de la información relacionados con la plataforma (procedimientos, políticas, etc.) y en los relativos al funcionamiento y normas de uso de los servicios que se pongan a disposición de los usuarios apoyados en la solución.
79. Será responsabilidad de la organización donde se implante la solución LORETO-NG el disponer de la normativa interna y de los procedimientos y/o herramientas a tal efecto.

4.27 [MP.INFO.6] Copias de Seguridad

80. El proceso de copias de seguridad de LORETO-NG se integrará con la solución de respaldo/*backup* adoptada en la organización donde se haya implantado, tanto a nivel de software de respaldo como de hardware especializado que se requiera.
81. Se puede realizar una copia de seguridad de todo el contenido almacenado, como únicamente de la base de datos de Nextcloud, siendo responsabilidad de la organización elegir las ventanas adecuadas para su realización.
82. Para realizar una copia de seguridad completa, se pararán todos los contenedores excepto el de la base de datos para poder realizar un volcado de los datos, integrándose el fichero obtenido en el proceso de copias de la organización. Se realizará asimismo copia de la carpeta "*loreto*" en la que se encuentran todos los contenedores *Docker*.

83. En aquellos elementos complementarios de la solución LORETO-NG, como es el caso de los equipos empleados para administración y monitorización del sistema, será de aplicación lo que determina el ENS para categoría ALTA.

4.28 [MP.S.1] Protección del Correo Electrónico

84. La solución LORETO-NG emplea el servicio de correo electrónico de la organización para la recuperación de contraseñas, la creación de usuarios y el envío de notificaciones.
85. En este sentido, es el servicio de correo que emplee la organización, ya sea este propio o externalizado, el que deberá protegerse mediante las disposiciones del ENS.

4.29 [MP.S.4] Protección frente a denegación de servicio

86. La protección de la solución LORETO-NG frente a ataques de denegación de servicio (DoS), incluyendo a los distribuidos (DDoS), es responsabilidad de la organización donde se implante, siempre que se considere el nivel de la dimensión disponibilidad como ALTO.
87. Se recomienda contratar la protección frente a ataques de denegación de servicio a la operadora que suministra la conexión a internet como un servicio de seguridad, aunque existen otras soluciones de protección basadas en medios propios (*appliances* especializadas).

5. CONFIGURACIÓN DE SEGURIDAD

88. Para dar respuesta a los requisitos establecidos en este Perfil de Cumplimiento Especifico para la solución de Cloud privado o comunitario, se deberá estar a lo dispuesto en el ENS para la medida de seguridad [op.exp.2] Configuración de seguridad, así como en el apartado 4.7 de este documento.
89. Si se opta por el uso de otras tecnologías para la aplicación de este Perfil de Cumplimiento Específico para LORETO-NG, será necesario que la configuración de seguridad haya sido previamente validada por el CCN.

6. SOLUCIONES DE SEGURIDAD COMPLEMENTARIAS

Pueden adoptarse soluciones complementarias a LORETO-NG basadas en herramientas del CCN.

6.1 Solución CARLA

Se trata de una solución orientada a la protección del dato en sí mismo, la cual es idónea para entornos de alojamiento en la Nube, en este caso en modelo de entrega de servicios como Cloud privada o comunitaria.

La solución CARLA refuerza diferentes medidas de seguridad de este Perfil de Cumplimiento Específico para LORETO-NG, las más relevantes de las cuales se detallan a continuación:

- **[op.acc.2] Requisitos de acceso**: permite proteger los documentos críticos mediante mecanismos que impidan su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Los privilegios de acceso a los documentos pueden diferenciarse por usuario o grupo de usuarios y con un control granular de permisos (ver, editar, copiar y pegar, etc.), esté la información donde esté, ya sea albergada en LORETO-NG o extraída en estaciones de trabajo, incluidos los dispositivos móviles.
- **[op.exp.8] Registro de actividad:** a través de CARLA se dispone de un registro de auditoría adicional, que identifica al usuario que ha accedido a un documento crítico, permisos, fecha y hora, tipo de evento (acceso realizado, desprotección, acceso bloqueado, etc.), etc.
- **[op.ext.3] Protección de la cadena de suministro:** CARLA permite mitigar el riesgo de pérdida, o fuga de información, ya que la documentación viaja protegida a través de una política de protección marcada por la organización y que se aplicará con independencia de que la documentación se encuentre en LORETO-NG o en los sistemas de un proveedor de la cadena de suministro de la organización.
- **[mp.com.2] Protección de la confidencialidad:** al estar la seguridad en CARLA basada en el dato y no en el perímetro, propicia que una posible exfiltración de datos no suponga una brecha de seguridad para la organización, al permanecer protegidos los documentos sustraídos sin autorización. El documento viaja etiquetado y se almacena cifrado en origen y destino, descifrándose de forma transparente únicamente si es permitido bajo el control de la política establecida.

PUBLICACIONES DE DEFENSA
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL