centro criptológico nacional

Guía de Cumplimiento Específico
CCN-STIC 889G

Perfil de Cumplimiento Específico Oracle Cloud SaaS
Servicio de Cloud Corporativo

JULIO 2023

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-184-1
Fecha de Edición: julio de 2023

CCN 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
2023.07.04 14:47:43 +02'00'

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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 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, 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.
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 los servicios contratados en la modalidad SaaS del Cloud de Oracle.**

2. TECNOLOGÍAS IMPLICADAS

7. Este perfil de cumplimiento podrá ser de aplicación en todas aquellas entidades cuyo sistema de información, tras un correcto proceso de categorización, obtenga unas necesidades de nivel ALTO o inferior; y los servicios de los que se componga dicho sistema de información se correspondan únicamente con los ofrecidos por la solución de Oracle Cloud Infrastructure (OCI), en su modalidad de despliegue como nube pública, ofreciendo servicios de software como servicio (SaaS) para Oracle Fusion Applications (OFA) y Oracle Enterprise Performance Management (EPM), según corresponda en cada solución contratada.

8. De acuerdo con lo establecido en la Guía de seguridad de las TIC CCN-STIC-823 Utilización de servicios en la Nube, se definen las nubes con modelos de despliegue públicos como aquellas cuya infraestructura es ofrecida al público general o a un gran grupo de industria, y dicha infraestructura es controlada por un proveedor de servicios en la nube.
9. Para la aplicación de este Perfil de Cumplimiento Especifico, la solución Cloud de Oracle ofrece servicios en cualquiera de las categorías cuyos sistemas son poseedores de la certificación de conformidad con el ENS en categoría Alta.

3. DECLARACIÓN DE APLICABILIDAD

10. La declaración de aplicabilidad es el conjunto de medidas que son de aplicación para el cumplimiento del ENS. El conjunto de medidas dependerá de los niveles asociados a las dimensiones de seguridad.
11. Se ha determinado que, para los servicios contratados en la modalidad SaaS de Oracle Cloud Infrastructure (OCI), las siguientes medidas de seguridad y su exigencia en el nivel de madurez se describen en la tabla siguiente, tanto aquellas que son de aplicación, como aquellas que no lo son:

Dimensiones						
Afectadas	Categoría Básica	Categoría Media	Categoría Alta			
				Control	Aplicación FUSION	Aplicación EPM
MARCO ORGANIZATIVO						
categoría	aplica	=	=	[org.1]	ALTO	ALTO
categoría	aplica	=	=	[org.2]	ALTO	ALTO
categoría	aplica	=	=	[org.3]	ALTO	ALTO
categoría	aplica	=	=	[org.4]	ALTO	ALTO
MARCO OPERACIONAL						
categoría	aplica	+ R1	+R2	[op.pl.1]	ALTO	ALTO
categoría	aplica	+ R1	+R1 +R2 +R3	[op.pl.2]	ALTO	ALTO
categoría	aplica	=	=	[op.pl.3]	ALTO	ALTO
D	aplica	+ R1	+R1	[op.pl.4]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.pl.5]	ALTO	ALTO
T A	aplica	+ R1	+R1	[op.acc.1]	ALTO	ALTO
C I T A	aplica	=	+R1	[op.acc.2]	ALTO	ALTO
C I T A	n.a.	aplica	+R3	[op.acc.3]	ALTO	ALTO
C I T A	aplica	=	=	[op.acc.4]	ALTO	ALTO
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	=	[op.acc.5]	ALTO	ALTO

Dimensiones						
Afectadas	Categoría Básica	Categoría Media	Categoría Alta			
				Control	Aplicación FUSION	Aplicación EPM
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	[op.acc.6]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.1]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.2]	ALTO	ALTO
categoría	aplica	+ R1	+ R1 + R2 + R3	[op.exp.3]	ALTO	ALTO
categoría	aplica	+ R1	+ R1 + R2	[op.exp.4]	ALTO	ALTO
categoría	n.a.	aplica	+ R1	[op.exp.5]	ALTO	ALTO
categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	[op.exp.6]	ALTO	ALTO
categoría	Aplica	+ R1 + R2	+ R1 + R2 + R3	[op.exp.7]	ALTO	ALTO
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	[op.exp.8]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.9]	ALTO	ALTO
categoría	aplica	+ R1	=	[op.exp.10]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.ext.1]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.ext.2]	ALTO	ALTO
categoría	n.a.	n.a	aplica	[op.ext.3]	ALTO	ALTO
categoría	n.a.	aplica	+ R1	[op.ext.4]	ALTO	ALTO
categoría	aplica	+ R1	+ R1 + R2	[op.nub.1]	ALTO	ALTO
D	n.a.	aplica	=	[op.cont.1]	n.a.	n.a.
D	n.a.	n.a.	aplica	[op.cont.2]	ALTO	ALTO
D	n.a.	n.a.	aplica	[op.cont.3]	n.a.	n.a.
D	n.a.	n.a.	aplica	[op.cont.4]	ALTO	ALTO
categoría	aplica	+ R1	+ R1 + R2	[op.mon.1]	ALTO	ALTO
categoría	aplica	+ R1 + R2	=	[op.mon.2]	ALTO	ALTO
categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6	[op.mon.3]	ALTO	ALTO
MEDIDAS DE PROTECCIÓN						
categoría	aplica	=	=	[mp.if.1]	n.a.	n.a.
categoría	aplica	=	=	[mp.if.2]	n.a.	n.a.
categoría	aplica	=	=	[mp.if.3]	n.a.	n.a.
D	aplica	+ R1	=	[mp.if.4]	n.a.	n.a.
D	aplica	=	=	[mp.if.5]	n.a.	n.a.
D	n.a.	aplica	=	[mp.if.6]	n.a.	n.a.

Dimensiones						
Afectadas	Categoría Básica	Categoría Media	Categoría Alta			
				Control	Aplicación FUSION	Aplicación EPM
categoría	aplica	=	=	[mp.if.7]	n.a.	n.a.
categoría	n.a.	aplica	=	[mp.per.1]	ALTO	ALTO
categoría	aplica	+ R1	=	[mp.per.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.3]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.4]	ALTO	ALTO
categoría	aplica	+ R1	=	[mp.eq.1]	ALTO	ALTO
A	n.a.	aplica	+ R1	[mp.eq.2]	ALTO	ALTO
categoría	aplica	=	+ R1 + R2	[mp.eq.3]	ALTO	ALTO
C	aplica	+ R1	=	[mp.eq.4]	ALTO	ALTO
categoría	aplica	=	=	[mp.com.1]	ALTO	ALTO
C	aplica	+ R1	+ R1 + R2 + R3	[mp.com.2]	ALTO	ALTO
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	[mp.com.3]	ALTO	ALTO
categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	[mp.com.4]	ALTO	ALTO
C	n.a.	aplica	=	[mp.si.1]	ALTO	ALTO
C I	n.a.	aplica	+ R1 + R2	[mp.si.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.si.3]	ALTO	ALTO
categoría	aplica	=	=	[mp.si.4]	ALTO	ALTO
C	aplica	+ R1	=	[mp.si.5]	ALTO	ALTO
categoría	n.a.	+ R1 + R2 + R3 + R4	=	[mp.sw.1]	ALTO	ALTO
categoría	aplica	+ R1	=	[mp.sw.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.info.1]	ALTO	ALTO
C	n.a.	aplica	=	[mp.info.2]	ALTO	ALTO
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	[mp.info.3]	n.a.	n.a.
T	n.a.	=	aplica	[mp.info.4]	n.a.	n.a.
C	aplica	=	=	[mp.info.5]	ALTO	ALTO
D	aplica	+ R1	+ R1 + R2	[mp.info.6]	ALTO	ALTO
categoría	aplica	=	=	[mp.s.1]	n.a.	n.a.
categoría	+ [R1 o R2]	=	+ R2 + R3	[mp.s.2]	ALTO	ALTO
categoría	aplica	=	+ R1	[mp.s.3]	ALTO	ALTO
D	n.a.	aplica	+ R1	[mp.s.4]	ALTO	ALTO

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

12. En la tabla anterior se han empleado las siguientes convenciones:

a) En cuanto a la aplicación de las dimensiones de seguridad, se tendrán en cuenta según las iniciales en mayúsculas:

i. Disponibilidad [D].

ii. Autenticidad [A].

iii. Integridad [I].

iv. Confidencialidad [C].

v. Trazabilidad [T].

b) En cuanto a la aplicación de las categorías según el marco de las medidas de seguridad a aplicar con respecto a la categoría básica, media o alta del ENS:

i. Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.

ii. La palabra "aplica" especifica que esta medida se aplica a partir del nivel para el que se establece.

iii. Las siglas "n.a." indican que la medida de seguridad para ese control no se aplica a ese nivel.

iv. Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida, pero que no siempre son incrementales entre sí.

v. Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por "o" [Rn o Rn + 1].

vi. El símbolo "=" indica que la medida se aplica con las mismas condiciones de seguridad que el nivel precedente.

13. En la columna Aplicación, la palabra ALTO indica que la medida aplica a la categoría alta del ENS.

3.1 MEDIDAS DE APLICACIÓN EN FUSION Y EPM

14. Las medidas de seguridad definidas en la tabla anterior, según en el Anexo II del RD 311/2022, disponen un total de 73 medidas de las cuales son de aplicación, para la modalidad SaaS de Oracle, las **61** siguientes:

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (31):

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento/gestión de la capacidad

[op.pl.5] Componentes certificados

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.3] Segregación de funciones y tareas

[op.acc.4] Proceso de gestión de derechos de acceso

[op.acc.5] Mecanismos de autenticación (usuarios externos)

[op.acc.6] Mecanismos de autenticación (usuarios de la organización)

[op.exp.1] Inventario de activos

[op.exp.2] Configuración de seguridad

[op.exp.3] Gestión de la configuración de seguridad

[op.exp.4] Mantenimiento y actualizaciones de seguridad

[op.exp.5] Gestión de cambios

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

[op.exp.7] Gestión de incidentes

[op.exp.8] Registro de la actividad

[op.exp.9] Registro de la gestión de incidentes

[op.exp.10] Protección de claves criptográficas

[op.ext.1] Contratación y acuerdos de nivel de servicio

[op.ext.2] Gestión diaria

[op.ext.3] Protección de la cadena de suministro

[op.ext.4] Interconexión de sistemas

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

[op.cont.2] Plan de continuidad

[op.cont.4] Medios alternativos

[op.mon.1] Detección de intrusión

[op.mon.2] Sistema de métricas

[op.mon.3] Vigilancia

Medidas de Protección (26):

[mp.per.1] Caracterización del puesto de trabajo

[mp.per.2] Deberes y obligaciones

[mp.per.3] Concienciación

[mp.per.4] Formación

[mp.eq.1] Puesto de trabajo despejado

[mp.eq.2] Bloqueo de puesto de trabajo

[mp.eq.3] Protección de dispositivos portátiles

[mp.eq.4] Otros dispositivos conectados a la red

[mp.com.1] Perímetro seguro

[mp.com.2] Protección de la confidencialidad

[mp.com.3] Protección de la integridad y de la autenticidad

[mp.com.4] Separación de flujos de información en la red

[mp.si.1] Marcado de soportes

[mp.si.2] Criptografía

[mp.si.3] Custodia

[mp.si.4] Transporte

[mp.si.5] Borrado y destrucción

[mp.sw.1] Desarrollo de aplicaciones

[mp.sw.2] Aceptación y puesta en servicio

[mp.info.1] Datos personales

[mp.info.2] Calificación de la información

[mp.info.5] Limpieza de documentos

[mp.info.6] Copias de seguridad

[mp.s.2] Protección de servicios y aplicaciones web

[mp.s.3] Protección de la navegación web

[mp.s.4] Protección frente a denegación de servicio

4. CRITERIOS DE APLICACIÓN DE MEDIDAS PARA FUSION Y EPM

4.1 [OP.ACC] CONTROL DE ACCESO

15. El conjunto de medidas “op.acc Control de acceso” se aplicarán en la categoría y nivel ALTO, con las siguientes particularidades:

    a) El cambio de las credenciales en el primer acceso será responsabilidad de los usuarios finales de la plataforma, por lo que deberá incluirse en las normas de uso de esta, haciendo mención expresa a que se deberá cambiar la contraseña en el primer acceso.

    b) Los mecanismos de autenticación provistos por Oracle a través del Servicio OCI IAM, para el aprovisionamiento de los entornos Oracle Fusion y Oracle EPM y las herramientas de seguridad provistas en las distintas consolas de gestión de las aplicaciones de la nube, se ajustan a los requisitos exigibles en el Esquema Nacional de Seguridad siempre y cuando sean configurados a tal efecto por la organización usuaria del servicio, con la particularidad de que cada usuario local debe habilitarse el uso del doble factor de autenticación en su perfil, no pudiendo ser realizado por un administrador, y debe ser mencionado en las normas de uso de la misma.

    c) Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por OCI no puedan ser aplicados, como en el caso de los equipos de administración del sistema, serán de aplicación estas medidas en la categoría y nivel ALTO.

16. Las configuraciones que deben ser aplicadas, quedan descritas en las guías de configuración segura de Oracle referenciadas en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.2 [OP.EXP.2] CONFIGURACIÓN DE SEGURIDAD

17. La medida establece una seguridad mínima, la cual implementa Oracle en sus recursos en el momento de su creación.

18. Los equipos, antes de su entrada en producción, deberán configurarse de tal forma que:

    a) Se retiren cuentas y contraseñas estándar.

    b) Se aplique la regla de mínima funcionalidad.

19. Se considera indispensable que el sistema no proporcione funcionalidades no requeridas, solo las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. La configuración será descrita en las correspondientes guías de configuración segura de Oracle y sus servicios relacionados que se referencian en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.3 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD

20. La medida establece que se deben registrar las actividades en el sistema, de forma que:
    a) Se genere un registro de auditoría, que incluya, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
    b) Se activen los registros de actividad en los servidores.
21. Los mecanismos para el registro de actividad de los usuarios provistos por Oracle son recogidos por los servicios de auditoría disponibles en las consolas de gestión de Oracle Fusion Aplications (OFA) y Oracle Enterprise Performance Management (EPM).
22. Esta medida se ajusta a los requisitos exigibles en el Esquema Nacional de Seguridad y debe ser aplicada por la organización usuaria de la nube a través de los servicios de Oracle mencionados, que serán detallados en las correspondientes guías de configuración segura de Oracle y sus servicios relacionados que se referencian en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.4 [OP.NUB.1] PROTECCIÓN DE SERVICIOS EN LA NUBE

23. Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten, en este caso, Software como servicio (Software as a Service, SaaS).
24. Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, en otros, requisitos relativos a la auditoría de pruebas de penetración (Pentesting), transparencia, cifrado y gestión de claves y jurisdicción de los datos.
25. Oracle dispone del Certificado de Conformidad con el Esquema Nacional de Seguridad y cumple con las medidas desarrolladas en las guías de seguridad CCN-STIC-XXX Guía de Configuración segura para Oracle SaaS Fusion Applications y CCN-STIC-XXX Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM.

4.5 [OP.CONT.2] PLAN DE CONTINUIDAD

26. Serán de aplicación las medidas de categoría y nivel ALTO para la dimensión de Disponibilidad del sistema, que cumpla con las acciones que establece la medida, siendo la organización responsable de la correcta implementación de estas medidas en función de las necesidades de uso de los servicios de Oracle, que se describen en las guías de configuración segura de Oracle referenciadas en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.6 [OP.CONT.4] MEDIOS ALTERNATIVOS

27. Esta medida se establece para un nivel de seguridad ALTO en la dimensión de Disponibilidad del sistema, indicando que estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo disfrutará de las mismas garantías de seguridad que el servicio habitual.
28. Oracle dispone de la infraestructura que garantiza la disponibilidad del servicio contratado ante los imprevistos recogidos en esta medida por el ENS, y dispone del Certificado de Conformidad con el Esquema Nacional de Seguridad para acreditarlo. Los mecanismos que garantizan esta continuidad de negocio serán descritos en las guías de Configuración segura de Oracle referenciadas en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.7 [OP.MON.3] VIGILANCIA

29. La medida establece que debe disponerse de un sistema automático de recolección de eventos de seguridad y, a su vez, dichos eventos de seguridad puedan ser correlacionados.
30. Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.
31. Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos. Además, debe ser capaz de detectar amenazas persistentes avanzadas (Advanced Persistent Threat, APT), mediante la detección de anomalías significativas en el tráfico de red.
32. Se dispondrá de observatorios digitales con fines de ciber vigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.
33. Para la minería de datos, el ENS establece la aplicación de medidas de prevención, detección y reacción frente a intentos de minería de datos, a través de limitar las consultas, monitorización de volumen y frecuencia y estableciendo alertas a los administradores de seguridad ante comportamientos sospechosos en tiempo real.
34. Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán inspecciones de seguridad para la verificación de configuración, análisis de vulnerabilidades y pruebas de penetración.

4.8 [MP.IF] MEDIDAS DE PROTECCIÓN DE INSTALACIONES E INFRAESTRUCTURAS

35. Serán de aplicación las medidas de categoría y nivel ALTO si se da la particularidad de enlazar el sistema Cloud mediante una arquitectura híbrida con el proveedor de servicios en la nube.

36. En el caso mencionado, será responsabilidad de la organización usuaria de los servicios, ajustarse a los requisitos exigibles en el Esquema Nacional de Seguridad para la protección de las instalaciones e infraestructuras locales conectadas a los servicios Cloud de Oracle.

4.9 [MP.EQ.2] BLOQUEO DE PUESTO DE TRABAJO

37. Dentro del conjunto de protección de los equipos, el bloqueo es la única medida que aplica al contemplar el puesto de trabajo como la sesión establecida a la nube de la organización, no como un puesto físico, por lo que se debe aplicar el bloqueo de la sesión e impedir el acceso no autorizado tras pasar un tiempo de inactividad.

38. Esta medida define un tiempo para la caducidad de la sesión y será responsabilidad de la organización usuaria su correcta configuración, cuya aplicación técnica será recogida por las guías de configuración segura de Oracle y sus servicios relacionados, referenciadas en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.10 [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN

39. Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema y recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el Artículo 40 y los criterios generales señalados en el Anexo I.

40. Esta medida se aplicará 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 Cloud, que se pongan a disposición de los usuarios.

41. El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido. Además, tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido en cada momento.

42. No será exigible la aplicación de esta medida en los documentos compartidos por los usuarios haciendo uso de los servicios Cloud.

4.11 [MP.INFO.3] FIRMA ELECTRÓNICA

43. Esta medida no será de aplicación siempre y cuando no se contemple el uso de la firma electrónica para funcionalidades relacionadas con el uso y/o administración, configuración o mantenimiento de la plataforma, y así sea considerado por el responsable de seguridad. No obstante, esta medida se encuentra fuera de ámbito en la infraestructura de Oracle y de los servicios Oracle Fusion Applications (OFA) y Oracle Enterprise Performance Management (EPM).

4.12 [MP.INFO.5] LIMPIEZA DE DOCUMENTOS

44. Esta medida solo se aplicará 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 Cloud, que se pongan a disposición de los usuarios, y será responsabilidad de la organización usuaria de la nube disponer de los procedimientos a tal efecto.

4.13 [MP.INFO.6] COPIAS DE SEGURIDAD

45. Esta medida establece que deben realizarse copias de seguridad que permitan recuperar datos perdidos de manera accidental o intencionadamente, con una antigüedad determinada por la normativa interna de la organización. Los procedimientos de respaldo establecidos indicarán la frecuencia de las copias, los requisitos de almacenamiento en el propio lugar, los requisitos de almacenamiento en otros lugares y los controles para el acceso autorizado a las copias de respaldo.

46. Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad. Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

4.14 [MP.S.1] PROTECCIÓN DEL CORREO ELECTRÓNICO

47. Esta medida no será de aplicación siempre y cuando no se contemple el uso del correo electrónico configurado en las cuentas de los usuarios, para tareas directamente relacionadas con la configuración y/o mantenimiento del sistema, y así sea considerado por el responsable de seguridad.

48. Oracle Cloud dispone del Servicio Email Delivery que ofrece con la conformidad exigida en el ENS en categoría Alta.

49. En caso de contemplar el uso del correo para los fines mencionados, y se empleará de forma interna para las notificaciones y alarmas de los sistemas de OCI, la responsabilidad de la correcta implementación y configuración del servicio Email Delivery recaerá en la organización usuaria del servicio.

5. CONFIGURACIÓN DE SEGURIDAD

50. Para dar respuesta a las medidas de seguridad identificadas en este Perfil de Cumplimiento Especifico usando la tecnología Oracle Fusion Applications (OFA) en la modalidad SaaS, se deberá consultar lo establecido en la guía de seguridad “CCN-STIC-XXX Guía de Configuración segura para Oracle SaaS Fusion Applications”.

51. Para dar respuesta a las medidas de seguridad identificadas en este Perfil de Cumplimiento Especifico usando la tecnología Oracle Enterprise Performance Management (EPM) en la modalidad SaaS, se deberá consultar lo establecido en la guía de seguridad “CCN-STIC-XXX Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM.

52. Si opta por el uso de otras tecnologías para la aplicación de este Perfil de Cumplimiento Especifico para Sistemas Cloud Corporativos, será necesario que la configuración de seguridad haya sido previamente validada por el CCN.

PUBLICACIONES Pd DE DEFENSA

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