centro criptológico nacional

Guía de Cumplimiento Específico
CCN-STIC 889

Perfil de Cumplimiento Especifico Oracle Cloud
Servicio de Cloud Corporativo

MARZO 2022

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2022.03.28 15:10:28 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-116-5

Fecha de Edición: marzo de 2022
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

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 3/2010, de 8 de enero, 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 3/2010, de 8 de enero, 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 el Cloud de Oracle en las modalidades IaaS y PaaS.**

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 Cloud de Oracle, tanto Oracle Cloud Infrastructure (OCI) en su modalidad de despliegue como nube pública, como Cloud at Customer (C@C) en su modalidad de despliegue como nube privada, y ofreciendo servicios de infraestructura como servicio (IaaS) y plataforma como servicio (PaaS), según corresponda en cada solución contratada.

8. De acuerdo a 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 el Cloud, tanto para OCI como para C@C, las medidas que son de aplicación o no y, en caso de aplicar, la exigencia en nivel de madurez de la medida, son las siguientes:

Dimensiones						
Afectadas	Cat.B	Cat.M	Cat.A			
				Org	Aplicación OCI	Aplicación C@C
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	+	++	[op.pl.1]	ALTO	ALTO
categoría	aplica	+	++	[op.pl.2]	ALTO	ALTO
categoría	aplica	=	=	[op.pl.3]	ALTO	ALTO
D	n.a.	aplica	=	[op.pl.4]	ALTO	ALTO
categoría	n.a.	n.a.	aplica	[op.pl.5]	ALTO	ALTO
A T	aplica	=	=	[op.acc.1]	ALTO	ALTO
I C A T	aplica	=	=	[op.acc.2]	ALTO	ALTO
I C A T	n.a.	aplica	=	[op.acc.3]	ALTO	ALTO
I C A T	aplica	=	=	[op.acc.4]	ALTO	ALTO
I C A T	aplica	+	++	[op.acc.5]	ALTO	ALTO
I C A T	aplica	+	++	[op.acc.6]	ALTO	ALTO
I C A T	aplica	+	=	[op.acc.7]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.1]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.2]	ALTO	ALTO

Dimensiones						
Afectadas	Cat.B	Cat.M	Cat.A			
				Org	Aplicación OCI	Aplicación C@C
categoría	n.a.	aplica	=	[op.exp.3]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.4]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.5]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.6]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.7]	ALTO	ALTO
T	aplica	+	++	[op.exp.8]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.9]	ALTO	ALTO
T	n.a.	n.a.	aplica	[op.exp.10]	ALTO	ALTO
categoría	aplica	+	=	[op.exp.11]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.ext.1]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.ext.2]	ALTO	ALTO
D	n.a.	n.a.	aplica	[op.ext.9]	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.
categoría	n.a.	aplica	=	[op.mon.1]	ALTO	ALTO
categoría	n.a.	n.a.	aplica	[op.mon.2]	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	+	=	[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.
categoría	aplica	=	=	[mp.if.7]	n.a.	n.a.
D	n.a.	n.a.	aplica	[mp.if.9]	n.a.	n.a.
categoría	n.a.	aplica	=	[mp.per.1]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.3]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.4]	ALTO	ALTO
D	n.a.	n.a.	aplica	[mp.per.9]	n.a.	n.a.
categoría	aplica	+	=	[mp.eq.1]	ALTO	ALTO
A	n.a.	aplica	+	[mp.eq.2]	ALTO	ALTO
categoría	aplica	=	+	[mp.eq.3]	ALTO	ALTO
D	n.a.	aplica	=	[mp.eq.9]	ALTO	ALTO
categoría	aplica	=	+	[mp.com.1]	ALTO	ALTO

Dimensiones						
Afectadas	Cat.B	Cat.M	Cat.A			
				Org	Aplicación OCI	Aplicación C@C
C	n.a.	aplica	+	[mp.com.2]	ALTO	ALTO
I A	aplica	+	++	[mp.com.3]	ALTO	ALTO
categoría	n.a.	n.a.	aplica	[mp.com.4]	ALTO	ALTO
D	n.a.	n.a.	aplica	[mp.com.9]	n.a.	n.a.
C	aplica	=	=	[mp.si.1]	ALTO	ALTO
I C	n.a.	aplica	+	[mp.si.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.si.3]	ALTO	ALTO
categoría	aplica	=	=	[mp.si.4]	ALTO	ALTO
C	aplica	+	=	[mp.si.5]	ALTO	ALTO
categoría	n.a.	aplica	=	[mp.sw.1]	ALTO	ALTO
categoría	aplica	+	++	[mp.sw.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.info.1]	ALTO	ALTO
C	aplica	+	=	[mp.info.2]	ALTO	ALTO
C	n.a.	n.a.	aplica	[mp.info.3]	ALTO	ALTO
I A	aplica	+	++	[mp.info.4]	n.a.	n.a.
T	n.a.	n.a.	aplica	[mp.info.5]	n.a.	n.a.
C	aplica	=	=	[mp.info.6]	ALTO	ALTO
D	aplica	=	=	[mp.info.9]	ALTO	ALTO
categoría	aplica	=	=	[mp.s.1]	n.a.	n.a.
categoría	aplica	=	+	[mp.s.2]	ALTO	ALTO
D	n.a.	aplica	+	[mp.s.8]	ALTO	ALTO
D	n.a.	n.a.	aplica	[mp.s.9]	n.a.	n.a.

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. El símbolo "+" establece que la medida se aplica a nivel medio, incrementándose la seguridad con respecto al anterior nivel.

v. El símbolo "++" refiere a que la medida se aplica a nivel alto, incrementándose la seguridad con respecto a los anteriores niveles.

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 OCI Y C@C

14. Las medidas de seguridad definidas en la tabla anterior, según en el Anexo II del RD 3/2010, disponen un total de 75 medidas de las cuales son de aplicación, tanto en OCI como en C@C, las **59** 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 (29):

[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 capacidades

[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] Mecanismo de autenticación
[op.acc.6] Acceso local (local log-on)
[op.acc.7] Acceso remoto (remote log-in)
[op.exp.1] Inventario de activos
[op.exp.2] Configuración de seguridad
[op.exp.3] Gestión de la configuración
[op.exp.4] Mantenimiento
[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 de los usuarios
[op.exp.9] Registro de la gestión de incidentes
[op.exp.10] Protección de los registros de actividad
[op.exp.11] Protección de claves criptográficas
[op.ext.1] Contratación y acuerdos de nivel de servicio
[op.ext.2] Gestión diaria
[op.ext.9] Medios alternativos
[op.cont.2] Plan de continuidad
[op.mon.1] Detección de intrusión
[op.mon.2] Sistema de métricas

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 equipos portátiles
[mp.eq.9] Medios alternativos
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.com.3] Protección de la autenticidad y de la integridad

[mp.com.4] Segregación de redes

[mp.si.1] Etiquetado

[mp.si.2] Criptografía

[mp.si.3] Custodia

[mp.si.4] Transporte

[mp.si.5] Borrado y destrucción

[mp.sw.1] Desarrollo

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

[mp.info.1] Datos de carácter personal

[mp.info.2] Calificación de la información

[mp.info.3] Cifrado

[mp.info.6] Limpieza de documentos

[mp.info.9] Copias de seguridad (backup)

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

[mp.s.8] Protección frente a la denegación de servicio

4. CRITERIOS DE APLICACIÓN DE MEDIDAS PARA OCI Y C@C

4.1 [OP.ACC] CONTROL DE ACCESO

15. El conjunto de medidas “op.acc Control de acceso” será de aplicación 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 la misma, 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, 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.

d) En C@C, será de aplicación la medida en la categoría y nivel ALTO para el acceso remoto directo a los sistemas Exadata por parte de los usuarios, sin utilizar la consola de la nube.

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, solamente 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 DE LOS USUARIOS

20. La medida establece que se deben registrar las actividades de los usuarios del sistema, de forma que se guarde:
    a) Quién realiza la actividad, cuándo la realiza y sobre qué.
    b) La actividad de los usuarios y especialmente la de los operadores y administradores del sistema en el momento en que pueden acceder a la configuración y actuar en el mantenimiento del mismo.
    c) Las actividades realizadas con éxito, así como los intentos infructuosos.
21. Los mecanismos para el registro de actividad de los usuarios provistos por Oracle son:
    a) En OCI, serán recogidos por los servicios Audit y Data Safe.
    b) En C@C, serán recogidos por los servicios Audit, Data Safe y Unified Auditing.
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.EXP.10] PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

23. Esta medida aplica únicamente a la categoría alta del ENS, debiendo implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:
    a) Determinar el período de retención de los registros.
    b) Asegurar fecha y hora.
    c) Permitir el mantenimiento de los registros, sin que estos puedan ser alterados o eliminados por personal no autorizado.
    d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.
24. De acuerdo con las indicaciones del CCN, se articulan los mecanismos para garantizar la disponibilidad y retención de los registros, así como los procedimientos operativos para su salvaguarda.
25. Oracle Cloud dispone del Servicio Audit que tiene establecida una retención para los registros de actividad de 365 días. Si fuera necesario disponer de más retención, el cliente deberá realizar una petición al servicio de soporte My Oracle Support (MOS), proceso que será descrito en las guías de configuración segura de Oracle y sus servicios relacionados, referenciadas en el punto 5 CONFIGURACIÓN DE SEGURIDAD de este documento.

4.5 [OP.EXT.9] MEDIOS ALTERNATIVOS

26. 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.
27. 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.

4.6 [OP.CONT.2] PLAN DE CONTINUIDAD

28. 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.

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

29. Serán de aplicación las medidas de categoría y nivel ALTO si se da alguna de las siguientes particularidades:
    a) En OCI, si el sistema Cloud se enlaza mediante una arquitectura híbrida con el proveedor de servicios en la nube.
    b) En C@C, si el sistema Cloud se enlaza mediante la contratación del servicio de Cloud at Customer del proveedor de servicios en la nube.
30. La medida “mp.if.9 Instalaciones Alternativas”, solo será de aplicación cuando se haya valorado la dimensión de disponibilidad como ALTO, y siempre tomando en consideración las soluciones de redundancia disponibles en las instalaciones que ofrece el proveedor de servicio Cloud, el cual dispone de conformidad con el ENS en categoría Alta.
31. En los casos mencionados, 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.

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

32. 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.
33. 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.

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

34. 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 43 y los criterios generales prescritos en el Anexo I.
35. 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.
36. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido.

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

38. OCI dispone de varios servicios para la protección de datos en las Bases de datos, con los que aplicar medidas de protección de acceso a datos confidenciales, y serán descritas en 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.3] CIFRADO

39. Para el cifrado de información se determinará su dimensión en cuanto a la confidencialidad de la medida para la categoría y nivel ALTO, con la siguiente particularidad:

    a) La información se cifrará tanto durante su almacenamiento como durante su transmisión. La información sólo estará descifrada mientras se está haciendo uso de ella.

40. Oracle cumple con la norma utilizando la criptografía para las comunicaciones que establece el ENS, así como para los soportes de la infraestructura, disponiendo de la correspondiente certificación del CCN que lo acredita.

4.11 [MP.INFO.4] FIRMA ELECTRÓNICA

41. 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.

4.12 [MP.INFO.6] LIMPIEZA DE DOCUMENTOS

42. 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.9] COPIAS DE SEGURIDAD (BACK-UP)

43. Esta medida establece la necesidad de realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Además, estas copias deben disponer del mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se exige que las copias de seguridad estén cifradas para garantizar la confidencialidad.

44. Las copias de seguridad deberán abarcar la Información de trabajo de la organización, las aplicaciones en explotación, incluyendo los sistemas operativos, los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga y las claves utilizadas para preservar la confidencialidad de la información, siendo responsable la organización de su planificación e implantación.

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

45. 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.
46. Oracle Cloud dispone del Servicio Email Delivery que ofrece con la conformidad exigida en el ENS en categoría Alta.
47. En caso de contemplar el uso del correo para los fines mencionados, y se utilizara 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

48. Para dar respuesta a las medidas de seguridad identificadas en este Perfil de Cumplimiento Especifico usando la tecnología Oracle Cloud Infrastructure (OCI) en cualquiera de sus modalidades IaaS o PaaS, se deberá consultar lo establecido en las guías de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”, “CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión” y “CCN-STIC-889C Guía de Configuración segura para Arquitecturas Híbridas” para aplicar las configuraciones indicadas en dichos documentos.
49. Además, en el caso de implementar o disponer de recursos o instancias de Base de datos debe consultar la siguiente guía de seguridad “CCN-STIC-889D Guía de Configuración segura para OCI Database - Instancias VM”, y si implementa o dispone de equipos de Cómputo, debe consultar la siguiente guía de seguridad “CCN-STIC-889E Guía de Configuración segura para OCI Compute - Instancias VM y Bare Metal”.
50. Para dar respuesta a las medidas de seguridad identificadas en este Perfil de Cumplimiento Especifico usando la tecnología Cloud at Customer (C@C), debe consultar la siguiente guía de seguridad “CCN-STIC-889F Guía de Configuración segura para C@C Sistemas Exadata - Autonomous DB”.
51. 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 DE DEFENSA

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