centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 857

Requisitos de seguridad para Aplicaciones de Cibersalud en el contexto del ENS

Septiembre 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.09.21 15:33:04 +02'00'

NIPO: 083-20-108-5

Fecha de Edición: septiembre de 2020

Este documento se basa en material proporcionado por la Bundesamt für Sicherheit der Informationstechnik (BSI). El Sr. Carlos Galán ha participado en la redacción de este documento que también ha contado con la colaboración en su revisión de Sidertia Solutions S.L.

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

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 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.

septiembre de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

INDICE

1. INTRODUCCIÓN

1.1 TEMÁTICA Y DESTINATARIOS DE LA GUÍA

Desde la irrupción mundial de los dispositivos móviles en la actividad cotidiana de los ciudadanos, el uso de las **aplicaciones móviles relacionadas con la salud**, desde sus diferentes acercamientos (para profesionales, usuarios, proveedores, centros sanitarios, etc.), se ha extendido de tal forma que, independientemente de sus funcionalidades y beneficios, se hace necesario considerar, de manera formal y rigurosa, su seguridad.

Como decimos, estas aplicaciones están destinadas a colaborar en la **detección, diagnóstico, vigilancia y tratamiento** de una enorme variedad de patologías que, por su propia naturaleza, poseen importantes exigencias de seguridad en relación con la **disponibilidad** de los servicios implicados o la **confidencialidad, integridad, trazabilidad** o **autenticidad** de la información tratada.

Consciente de esta problemática y de su vínculo con el sector público y con los ciudadanos, últimos destinatarios de los esfuerzos sanitarios públicos, el Centro Criptológico Nacional (CCN) publica la presente *Guía CCN-STIC Requisitos de Seguridad para Aplicaciones de Cibersalud*, en el marco de lo dispuesto por el Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** (**ENS**, en adelante), sobre la base de un trabajo previo del *Bundesamt für Sicherheit in der Informationstechnik* (BSI)[1].

Nota importante:

Esta Guía está fundamentalmente dirigida a los fabricantes de aplicaciones de salud para dispositivos móviles, incluyendo el tratamiento y almacenamiento de datos sensibles, recogiendo las Mejores Prácticas sobre la materia.

1.2 OBJETIVO DE LA GUÍA

La digitalización de todos los ámbitos de la vida -ya sea en el trabajo, en el entorno doméstico, en el ocio, etc.-, sigue avanzando. A mediados de 2020, el número de usuarios de Internet superaba los cuatro mil ochocientos millones de personas[2]. De la población mundial actual (7.800 millones), dos tercios utilizan un smartphone, más de

[1] Oficina Federal de Seguridad de la Información alemana: *Sicherheitsanforderungen an digitale Gesundheitsanwendungen Technische Richtlinie* BSI TR-03161. (Trial Use, 2020)
[2] https://www.internetworldstats.com/stats.htm

3.000 millones de personas utilizan las redes sociales y el 90% de ellas lo hacen desde su dispositivo móvil (*smartphone* o *tablet*). Este desarrollo está igualmente presente en el sistema de atención sanitaria, con una clara tendencia al "autodiagnóstico" y demandando al mismo tiempo un uso eficiente y respetuoso de los datos de salud tratados, siendo imprescindible posibilitar el acceso a los registros médicos, independientemente del momento y el lugar.

Como es sabido, las aplicaciones móviles relacionadas con la salud (a las que denominaremos **aplicaciones de Cibersalud**) tratan un importante cúmulo de datos personales, muchos de ellos de los denominados *categorías especiales de datos* o datos considerados sensibles[3], desde registros de frecuencia cardíaca y ritmo de sueño hasta tratamientos o planes de medicación, así como recetas médicas y certificados, además de facilitar en muchos casos la conexión del usuario con los servicios sanitarios correspondientes, actuando como nodos de comunicación. Así las cosas, un smartphone comprometido puede dejar en evidencia multitud de datos de la "vida digital" del usuario, algunos de los cuales pueden ser especialmente confidenciales.

El mantenimiento de la conformidad con la regulación de seguridad vigente -como el ENS, cuando sus ámbitos subjetivo y material de aplicación comprenda también el uso de dispositivos móviles-, puede dificultar considerablemente esta situación de riesgo de exposición y, en muchos casos, impedirla. Ya desde las fases de diseño y ulterior desarrollo, los fabricantes deben planificar meticulosamente cómo una aplicación móvil procesará, almacenará y protegerá los datos personales y otros datos sensibles de sus usuarios[4].

Como es sabido, la seguridad de la información, desde el punto de vista del ENS, contempla cinco dimensiones de protección: *Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad.* Obvio resulta mencionar que el cumplimiento de estos requisitos es particularmente importante en las aplicaciones móviles de salud. A diferencia del sector financiero, en donde los bancos pueden devolver a los clientes el dinero transferido fraudulentamente; en el sector sanitario, la confidencialidad de los datos sanitarios que se revelan de manera involuntaria se pierde definitivamente, y aunque el usuario pueda percibir una compensación o indemnización por ello, la divulgación no puede deshacerse. Además, la divulgación no

[3] *Categorías especiales de datos*, en la terminología del Reglamento (UE) 2016/679 (RGPD): "Datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física." (Art. 9).

[4] *Seguridad y Privacidad desde el diseño*, en términos del Reglamento (UE) 2016/679 (RGPD). Véase la *Guía de Privacidad desde el Diseño*, AEPD (oct. 2019)

consentida de datos sanitarios, tanto en el entorno social como en el profesional, puede tener consecuencias y repercusiones extraordinariamente importantes. Por ejemplo, la manipulación (ataque a la integridad) por parte de un atacante de los datos de salud de un tercero, podría tener un impacto significativo en las decisiones de tratamiento y, en última instancia, en la salud y en la vida de la persona.

La presente Guía tiene como objetivo ayudar a los desarrolladores de aplicaciones de Cibersalud a elaborar aplicaciones móviles seguras.

1.3 DESCRIPCIÓN GENERAL DE LA GUÍA

1.3.1 METODOLOGÍA

El término *aplicación*[5], tal como se utiliza en el presente documento, se refiere a una aplicación móvil de Cibersalud que puede funcionar de forma autónoma en una aplicación móvil en el dispositivo móvil o en combinación con un *backend* seguro. El término *backend*, tal como se utiliza en este documento, incluye también las plataformas de computación en la nube.

Debido al constante progreso, crecimiento y diversidad de los dispositivos móviles y sus plataformas, esta Guía no pretende ser exhaustiva. En vez de ello, persigue evidenciar los **requisitos mínimos exigibles para el funcionamiento seguro de una aplicación de salud.**

La presente Guía incluye lo que se ha denominado una ***Definición del Problema de Seguridad*** *(DPS),* que identifica los posibles escenarios de amenaza. Por tanto, los **objetivos de seguridad** de las aplicaciones móviles, sus plataformas y/o entornos de despliegue serán consecuencia de la DPS, y perseguirán prevenir las amenazas y mitigar los riesgos. Los diferentes escenarios de amenaza y los objetivos de seguridad señalados en esta Guía se basan en la experiencia que el CCN ha venido adquiriendo a lo largo de los años, en su colaboración con otras instituciones nacionales e internacionales homólogas, en las Guías CCN-STIC del CCN y en otros documentos europeos[6] e internacionales[7].

[5] NISTIR 7695 under Application ISO/IEC 19770-2: "A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously."

[6] European Union Agency for Network and Information Security, "Smartphone Secure Development Guidelines".

[7] The OWASP Foundation, "Mobile Security Testing Guide (MSTG)" y "Mobile AppSec Verification Standard".

Un requisito básico en las aplicaciones de Cibersalud, además de la conformidad con la legislación aplicable, pasa por la observancia de las que se consideran *mejores prácticas,* así como otros requisitos generales para aplicaciones seguras, lo que incluye la realización de rigurosas e intensivas pruebas funcionales y de integración y, en particular, pruebas positivas/negativas de las características de seguridad de la aplicación. La presente Guía identifica también requisitos adicionales y específicos.

1.3.2 TERMINOLOGÍA

Los términos utilizados en esta Guía tienen los siguientes significados:

- **DEBE**: El fabricante debe implementar una cierta propiedad como requisito obligatorio.
- **NO DEBE**: La aplicación/*backend* no debe, en ninguna circunstancia, poseer una cierta propiedad o evidenciar un comportamiento dado.
- **DEBERÍA**: La aplicación/*backend* debería tener una cierta propiedad o evidenciar un comportamiento dado, a menos que se demuestre que su ausencia no supone un riesgo para la seguridad de la operación o que su implementación no es actualmente posible debido a limitaciones técnicas.
- **PUEDE**: La aplicación/*backend* puede tener una cierta propiedad, que debe ser señalada por el proveedor de la solución.

1.4 PRUEBA DE CONCEPTO

La presente Guía se publica como un *documento vivo* al que se confiere el estatus de "Prueba de Concepto". Esto significa que, aunque se han definido objetivos de seguridad, aún no se ha adquirido suficiente experiencia en la aplicación de tales objetivos. Durante esta Prueba de Concepto, el CCN recabará la retroalimentación de la industria, lo que podría comportar adiciones, eliminaciones o modificaciones de los objetivos de seguridad señalados, que incorporarán en versiones sucesivas de esta Guía.

Además, futuras versiones se complementarán con capítulos que permitan la realización de pruebas y la Certificación de Conformidad con el ENS de los sistemas de información implicados en el desarrollo y explotación de las aplicaciones de Cibersalud.

2. VISIÓN GENERAL DE LOS REQUISITOS DE SEGURIDAD DE LAS APLICACIONES MÓVILES

2.1 CONCEPTOS DE APLICACIÓN EN LOS DISPOSITIVOS MÓVILES

El término "aplicación móvil" se refiere a un programa que se ejecuta en una plataforma móvil. Tales aplicaciones pueden dividirse generalmente en tres categorías:

- **Aplicaciones nativas** (epígrafe 2.1.1), cuya totalidad de código fuente se ejecuta en el cliente (dispositivo móvil en este caso).
- **Aplicaciones web** (epígrafe 2.1.2), cuya totalidad de código fuente (salvo el código de presentación) se ejecuta en el servidor web, y es el navegador el que recupera el resultado de las operaciones y las representa al usuario.
- **Enfoques híbridos** (epígrafe 2.1.3), cuyo código fuente se encuentra repartido entre el cliente y el servidor.

Puesto que el uso de las aplicaciones web se extiende más allá de los dispositivos móviles, la presente Guía se centra en las aplicaciones nativas y en la parte nativa de los enfoques híbridos[8].

2.1.1 APLICACIONES NATIVAS

Una aplicación nativa se adapta a una plataforma y a su sistema operativo, y está basada en las herramientas de desarrollo de software (*Software Development Kits - SDK*) integradas en la propia plataforma (tales como Android o iOS), proporcionando acceso directo a los componentes del dispositivo, tales como la función GPS, la cámara o el micrófono.

Debido a su cercanía al sistema operativo, este tipo de software suele exhibir un buen rendimiento, alta fiabilidad y un funcionamiento intuitivo, instalándose habitualmente desde la propia tienda de aplicaciones de la plataforma, pudiendo, a menudo, ejecutarse sin conexión.

Pese a ello, también hay desventajas asociadas con la proximidad al sistema operativo. Las actualizaciones del sistema operativo, por ejemplo, pueden requerir la adaptación de la aplicación si se desea mantener su funcionalidad. Este tipo de aplicaciones,

[8] Información adicional sobre el desarrollo y funcionamiento seguro de aplicaciones web puede encontrarse en la Guía CCN-STIC 412 Requisitos de seguridad en entornos y aplicaciones Web, Guía CCN-STIC 422 Desarrollo seguro de aplicaciones web, Guía CCN-STIC 812 ENS: Seguridad en entornos y aplicaciones web. Puede consultarse también el documento *OWASP Application Security Verification Standard.*

además, no puede instalarse en otros sistemas operativos: si la misma aplicación ha de ejecutarse en distintos sistemas operativos, debe escribirse un código separado para cada uno de ellos[9], lo que constituye una exigencia compleja y costosa.

2.1.2 APLICACIONES WEB

Como es sabido, las aplicaciones web son *websites* que están diseñados para percibirse y comportarse como una aplicación nativa, aunque, a diferencia de estas, las aplicaciones web no se basan en el SDK de la plataforma subyacente, sino en herramientas de programación clásicas utilizadas para el desarrollo web (HTML5 y JavaScript, por ejemplo), lo que hace que solo permitan un acceso muy limitado a los componentes del dispositivo.

Pese a todo, su mayor ventaja es que son independientes del sistema operativo. Puesto que las aplicaciones son accedidas desde un navegador web, pueden utilizarse de la misma forma en cualquier plataforma sin necesidad de realizar ningún ajuste a nivel de código.

2.1.3 ENFOQUES HÍBRIDOS

Las aplicaciones híbridas combinan las ventajas y los inconvenientes de las aplicaciones nativas y web. Con un SDK se crea una aplicación marco (*framework*), con todas las características de las aplicaciones nativas: puede acceder a los componentes del dispositivo y suele estar disponible en las tiendas de aplicaciones, aunque no puede instalarse en otras plataformas sin modificar el código fuente.

La aplicación marco (*framework*) realiza peticiones HTTP a un servidor web que contiene la lógica de negocio y la seguridad, con el fin de realizar acciones y recuperar datos y presentarlos al usuario.

2.2 SERVICIOS DE *BACKEND*

La mayoría de las aplicaciones no dependen únicamente de los recursos proporcionados por el entorno de ejecución para procesar y almacenar datos, sino que suelen trasladar estas tareas a un sistema central en *background* (*backend*). Estos sistemas no sólo procesan y almacenan datos, sino que, frecuentemente, también realizan tareas de autenticación y autorización de usuarios, así como otras actividades centralizadas.

[9] Otro enfoque es el concepto de "*cross-platform*" que se sustenta en el desarrollo simultáneo de una aplicación para diferentes plataformas, lo que no hace sino trasladar la dependencia a un middleware muy complejo, que debe cubrir todas las plataformas de destino.

Todo ello significa que no todas las funcionalidades de la aplicación deben implementarse necesariamente en los dispositivos móviles, sino que, muy frecuentemente, se limitan a desarrollar una interfaz gráfica de usuario (*frontend*). Cada aplicación tiene sus propias características en relación con la funcionalidad implementada en la propia aplicación o en un servidor externo.

Obviamente, se necesita una conexión activa a Internet para el uso de aplicaciones conectadas a un *backend*. La comunicación entre el *frontend* y el *backend* se realiza normalmente a través de una conexión segura HTTPS. El uso de los sistemas de *backend* no se limita a las aplicaciones móviles, sino que se suele utilizarse en muchos otros tipos de aplicaciones.

Puesto que la presente Guía se centra en las aplicaciones móviles, los siguientes epígrafes se refieren a la seguridad de la aplicación y, adicionalmente, sólo a aquellas características del *backend* que afectan directamente a dicha seguridad[10].

2.3 DEFINICIÓN DEL PROBLEMA DE SEGURIDAD

Hemos denominado ***Definición del Problema de Seguridad*** al conjunto de **Supuestos [A]**, **Amenazas [T]** y **Políticas de Seguridad [P]** que son relevantes para la seguridad de las aplicaciones de Cibersalud.

2.3.1 SUPUESTOS [A]

Concepto	Descripción
[A.Dispositivo]	Se refiere a la plataforma en la que se utiliza la aplicación, operada por el propio usuario, y protegida contra vulnerabilidades. Por ejemplo, mediante la instalación regular de los parches de seguridad del sistema operativo. Además, su seguridad no se ha visto comprometida por la ejecución deliberada de *'roots'* o *'jailbreaks'*[11].

[10] Para obtener información más detallada sobre el funcionamiento y el desarrollo seguros de los sistemas de *backend*, puede consultarse el texto introductorio *'Top 10 Web Application Security Risks'* de la OWASP Foundation. Por su parte, los usuarios de sistemas Cloud pueden consultar la Guía CCN-STIC 823 ENS: Seguridad en entornos Cloud o el documento de la BSI 'Cloud Computing Compliance Criteria Catalogue (C5)'.

[11] Ambos comportamientos (véase Guía CCN-STIC 827 *Gestión y uso de dispositivos móviles*) suponen una relajación de las funcionalidades de seguridad inherentes al sistema operativo, mediante la concesión de derechos de acceso de mayor nivel y la habilitación para la instalación de aplicaciones de fuentes desconocidas.

2.3.2 AMENAZAS [T]

Concepto	Descripción
[T.AccesoLocal]	Acceso no autorizado a datos sensibles de la aplicación, tales como datos no cifrados almacenados en el sistema de archivos o en la memoria; o también el acceso a datos sensibles cifrados en texto plano, tras haber analizado el mecanismo de cifrado.
[T.AccesoRemoto]	Acceso no autorizado a los datos sensibles del *backend* y a los activos y aplicaciones del usuario (por ejemplo, a través de la ruptura de una conexión TLS). Esto puede ocurrir, por ejemplo, por un mal uso de la aplicación móvil o por una vulnerabilidad en la implementación de la interfaz del *backend* en dirección al *frontend*.
[T.Autenticación]	Acceso a datos sensibles de otros usuarios con una identificación de usuario falsa o utilizando credenciales de grupo.
[T.Interceptación]	Interceptación o interferencia en la comunicación de la aplicación usando una conexión débilmente cifrada o no autenticada, o estableciendo una conexión de transporte con un componente no autorizado, debido, por ejemplo, a una insuficiente verificación de las propiedades del certificado.
[T.Costes]	La aplicación origina al usuario costes adicionales no previstos.
[T.Integridad]	Manipulación no autorizada y no detectada de los datos, en la memoria del dispositivo o en tránsito.
[T.Descubrimiento]	Descubrimiento de las contraseñas (por ejemplo, por *fuerza bruta*[12]), y obtener acceso no autorizado a datos sensibles de otro usuario.
[T.Memoria]	Realización de ingeniería inversa en la aplicación, descubriendo en la memoria estructuras de datos desprotegidas, de modo que se pueda acceder a las credenciales, claves o datos sensibles.
Ataque a la base de datos	Debido a una mala implementación de los servidores y sus consultas, los datos de los usuarios pueden ser accedidos por atacantes u otros usuarios.
Compartición de los datos	La aplicación, debido a una falta de revisión en la asignación de roles y en la comprobación de si un usuario accede únicamente a sus datos, puede revelar información no debida.
Debilidad en el	Los sistemas de reinicio de contraseña si no implementa un

[12] Ensayo y error.

reinicio de contraseñas	robusto sistema de validación puede provocar el reinicio de la contraseña de un usuario o el robo de la cuenta de un usuario legítimo.

2.3.3 POLÍTICAS DE SEGURIDAD [P]

[P.Autorización]	El fabricante desarrolla e implementa un concepto de autorización que controla los accesos de lectura y escritura a los datos sensibles. Los permisos de acceso deben fijarse de tal manera que sólo se concedan los derechos necesarios para satisfacer la finalidad principal de la aplicación. El concepto de autorización debe aplicarse independientemente de la autenticación.
[P.*Backend*Log]	La información relativa a todas las conexiones salientes se recoge en el *backend* para permitir realizar un análisis *post-mortem* de los incidentes de seguridad, incluida la meta-información sobre los *proxies* utilizados y los certificados de los servidores verificados.
[P.ActCriticas]	El fabricante monitoriza permanentemente la aplicación, los *frameworks* y las librerías, en busca de vulnerabilidades explotables[13], proporcionando una actualización en el corto plazo si se identifican tales vulnerabilidades. El *backend* debe informar a la aplicación sobre la actualización y, tras un periodo de tiempo definido, dejar de utilizar la aplicación.
[P.LibIn]	Los datos obtenidos de librerías de terceros o por el usuario deben validarse antes de ser utilizados por la aplicación (por ejemplo, validación de esquemas XML, comprobación de codificación inválida, etc.). El objetivo es proteger la aplicación de ataques derivados de entradas de datos dañinas. Los datos de entrada deben ser analizados por librerías especializadas en el análisis de los datos ante ataques conocidos como son los XSS o las inyecciones de código.
[P.LibOut]	La aplicación no debe enviar datos sensibles en texto plano a *frameworks* o librerías de terceros. Se permite el uso de los

[13] En desarrollo de software, un *framework* entorno de trabajo es una estructura conceptual y tecnológica, compuesta normalmente de artefactos o módulos concretos de software, que puede servir de base para la organización y desarrollo de software. Típicamente, puede incluir soporte de programas, librerías, y un lenguaje interpretado, entre otras herramientas de ayuda al desarrollo y de integración de los diferentes componentes de un proyecto. Un *framework* de terceros puede entenderse como un contenedor de funcionalidades que no ha sido creado bajo el control del desarrollador de la aplicación y que tampoco forma parte de la funcionalidad de la plataforma del sistema operativo utilizado.

	frameworks y librerías adecuados para proteger un canal de comunicación o un contenedor de almacenamiento local.
[P.Random]	Los números aleatorios deben obtenerse usando un generador de alta entropía[14]. La aplicación introducirá inicialmente la entropía del usuario en el generador de números aleatorios de la plataforma. A continuación, la aplicación obtendrá los números aleatorios del *backend* y los introducirá en el generador de números aleatorios local. Esto aplica únicamente a operaciones de carácter sensible como la criptografía, para un uso en operaciones de poca relevancia o de presentación, el generador por defecto es suficiente.
[P.Finalidad]	Toda recopilación, procesamiento, almacenamiento y transferencia de datos sólo puede llevarse a cabo con una finalidad definida y limitada. A tal efecto, el fabricante debe publicar la finalidad principal de la aplicación, qué datos se procesan, y cómo, dónde y cuánto tiempo se almacenan. En base a la finalidad principal, se debe seleccionar el comportamiento de comunicación permisible y la tecnología de sensores internos y externos utilizada. Nota/Ejemplo: Los datos de rastreo o localización, como el WiFi-SSID, el GPS, y otros similares, sólo pueden utilizarse para la finalidad prevista, bajo el principio de minimización de datos y custodiados adecuadamente. No se permite la permanencia de esos datos en el dispositivo (por ejemplo, en las grabaciones de imágenes), a menos que la finalidad prevista lo requiera directamente.

2.3.4 RIESGOS RESIDUALES

El funcionamiento de las aplicaciones de Cibersalud está sujeto a requisitos particularmente exigentes, que no pueden ser totalmente satisfechos usando los dispositivos y las soluciones en la nube existentes. Por este motivo, se identifican seguidamente algunos riesgos residuales:

- Los dispositivos móviles son susceptibles de ser sustraídos.
- La arquitectura abierta de muchas plataformas facilita el uso de malware.
- Las aplicaciones instaladas pueden explotar vulnerabilidades existentes.

[14] En Teoría de la Información, la *entropía* de una variable aleatoria es el nivel medio de "información", "sorpresa" o "incertidumbre" inherente a los posibles resultados de dicha variable. (Wikipedia). Un sistema con baja entropía es más predecible que un sistema con alta entropía.

- Un desafío particular es la protección de la información durante el procesamiento en la memoria principal.
- La instalación del *backend* en proveedores públicos de servicios *cloud* entraña riesgos especiales para los datos sensibles de los usuarios. Si bien el uso de comunicaciones seguras y los métodos de cifrado mitigan los riesgos, los datos están prácticamente desprotegidos durante el procesamiento en la nube. Esto impone exigencias extremadamente altas a los proveedores de servicios en la nube, así como a otros usuarios que pueden utilizar simultáneamente recursos de la misma máquina física.

  Efectivamente, un atacante que saliera de su máquina virtual podría acceder a otras máquinas virtuales (fuera de su propia área de cliente) y, por lo tanto, podría acceder y manipular datos sensibles de otro cliente (por ejemplo, los datos de salud de la aplicación).
- Las comunicaciones entre la plataforma, la aplicación y el *backend* están protegidas por un protocolo TLS, criptográficamente seguro. La presente Guía contempla una autenticación unilateral en la que la aplicación comprueba la autenticidad del *backend*. La aplicación añade su propia aleatoriedad al proceso de establecimiento de una conexión TLS a fin de dificultar que un atacante penetre en dicha conexión. Sin embargo, los números aleatorios en las plataformas de smartphones suelen carecer de la calidad necesaria para proteger los datos sensibles de una aplicación de Cibersalud. El riesgo residual durante el proceso de establecimiento de la conexión es que el atacante pueda falsificar la autenticidad de sus propios mensajes, lo que permitiría al atacante acceder y manipular los datos sensibles transmitidos desde la aplicación al *backend*. (La medida [O.Random_4] proporciona un medio que puede reducir este riesgo residual para la segunda conexión TLS, enriquecida con nueva entropía).

3. MEDIDAS DE SEGURIDAD PARA APLICACIONES DE CIBERSALUD

3.1 OBJETIVOS DE SEGURIDAD

Los siguientes objetivos deben considerarse **requisitos mínimos de seguridad** de las aplicaciones de Cibersalud, que deben ser satisfechos por los fabricantes de dichas aplicaciones.

Los **Objetivos de Seguridad** pueden dividirse en los siguientes tipos:

1. Prueba de la finalidad de la aplicación
2. Prueba de la arquitectura
3. Prueba del código fuente

4. Prueba del software de terceros
5. Prueba de la aplicación de la criptografía
6. Prueba de la autenticación
7. Prueba del almacenamiento y la protección de datos
8. Prueba de los recursos de pago
9. Prueba de las interacciones específicas de la plataforma
10. Prueba de la comunicación de red
11. Prueba de la resiliencia

Si la aplicación de Cibersalud utiliza una funcionalidad que debe protegerse, el fabricante debe documentar, para cada aspecto de la prueba, cómo se ha implementado la satisfacción del requisito.

Seguidamente, para cada uno de los objetivos señalados, se muestra su codificación, su descripción y su ubicación en el marco del Esquema Nacional de Seguridad (ENS-RD 3/2010)[15]. Independientemente de las medidas concretas que apliquen en cada caso, el fabricante deberá disponer siempre de una Política de Seguridad de la Información en relación con el sistema de información usado para el desarrollo de la aplicación de Cibersalud y para su explotación (medida [org.1] del ENS), así como haber realizado y mantener actualizado el correspondiente Análisis de Riesgos (artículo 13 y medida [op.pl.1] del ENS).

3.1.1 OBJETIVO (1): FINALIDAD DE LA APLICACIÓN

Concepto	Descripción	RD 3/2010 (ENS)
O.Finalidad_1	Antes de su instalación, el fabricante **DEBE** informar de la finalidad principal de la aplicación y de su *backend*, así como el uso de datos personales (por ejemplo, en la descripción ofrecida en la tienda de aplicaciones) e informar al usuario, al menos, en el momento de la primera puesta en funcionamiento.	Medidas [mp.info.1] y [mp.info.2], en relación con el art. 11 y la Disposición adicional primera de la LOPDGDD[16], sobre la base de los arts. 5, 6, 9 y 13 del RGPD[17].

[15] Una mención "No Determinado" o "N/D" significa que el requisito de seguridad no está específicamente contemplado en el ENS.
[16] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales.
[17] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD).

O.Finalidad_2	La aplicación y su *backend* **NO DEBEN** recopilar y procesar datos que no se correspondan con la finalidad perseguida para la finalidad principal de la aplicación.	Medidas [mp.info.1] y [mp.info.2], en relación con la Disposición adicional primera de la LOPDGDD, sobre la base de los arts. 5 y 6 del RGPD.
O.Finalidad_3	La aplicación y su *backend* **DEBEN** obtener el consentimiento explícito del usuario antes de recoger o procesar cualquier dato personal.	Medidas [mp.info.1] y [mp.info.2], en relación con los arts. 6 y 9 y la Disposición adicional primera de la LOPDGDD, sobre la base de los arts. 5, 6, 7 y 9 del RGPD.
O.Finalidad_4	Si el usuario no ha aceptado expresamente el uso de ciertos datos, éstos **NO DEBEN** ser utilizados por la aplicación o por el *backend*.	Medidas [mp.info.1] y [mp.info.2], en relación con el art. 5 y la Disposición adicional primera de la LOPDGDD, sobre la base del art. 9 del RGPD.
O.Finalidad_5	La aplicación y su *backend* **DEBEN** permitir al usuario retirar su consentimiento en cualquier momento, y **DEBE** informar sobre en qué forma esto podría alterar el comportamiento de la aplicación.	Medidas [mp.info.1] y [mp.info.2], en relación con la Disposición adicional primera de la LOPDGDD, sobre la base del art. 7 del RGPD.
O.Finalidad_6	El fabricante **DEBE** mantener un registro que muestre qué consentimientos del usuario se han obtenido. La parte específica del directorio del usuario **DEBE** ser visible también para el usuario.	Medidas [mp.info.1] y [mp.info.2], en relación con la Disposición adicional primera de la LOPDGDD, sobre la base del art. 7 del RGPD.
O.Finalidad_7	Si la aplicación o su *backend* utilizan frameworks o librerías de terceros, todas las funciones utilizadas de tales fuentes **DEBERÍAN** ser necesarias para la finalidad principal de la aplicación. La aplicación	Art. 16 y Medidas [mp.info.1] y [mp.info.2], en relación con el art. 5 y la Disposición adicional primera de la LOPDGDD, sobre la base de los arts.

	DEBERÍA deshabilitar de forma segura cualquier otra función.	5 y 6 del RGPD.
O.Finalidad_8	Los datos sensibles **NO DEBEN** ser compartidos con terceros a menos que sea necesario para la finalidad principal de la aplicación. La aplicación **DEBE** informar plenamente al usuario de las consecuencias de cualquier divulgación de los datos y obtener su consentimiento (OPT-IN). Nota: Si, por ejemplo, la aplicación utiliza la visualización de un mapa de un tercer fabricante, el usuario debe ser informado de que ciertos datos podrían ser transmitidos a terceros.	Medidas [mp.info.1] y [mp.info.2], en relación con el art. 11 y la Disposición adicional primera de la LOPDGDD, sobre la base de los arts. 5, 6, 9 y 13 del RGPD.
O.Finalidad_9	La aplicación **NO DEBE** mostrar datos sensibles en la pantalla a menos que sea necesario para la finalidad de la aplicación.	Medidas [mp.info.1] y [mp.info.2], en relación con el art. 11 y la Disposición adicional primera de la LOPDGDD, sobre la base de los arts. 5 y 13 del RGPD.
	Se debe comprobar el aislamiento de los usuarios. Un usuario accede únicamente a sus datos.	- Medida [op.acc.3] - Medida [op.acc.4] - Medida [mp.info.3]
	Todo envío de datos fuera de la aplicación, por mail o cualquier otro canal debe ir cifrado preferiblemente con sistemas de clave público-privada, en caso de imposibilidad con clave simétrica.	
	En el plan de pruebas de la aplicación se deben incluir pruebas de seguridad.	- Medida [mp.sw.1]
	Se debe auditar el código fuente de la aplicación y realizar pruebas de ataques de intrusión.	- Medida [mp.sw.2]

	La aplicación debe registrar los accesos del administrador y sus acciones sobre el aplicativo y los datos.	- Medida [op.acc.1] - Medida [op.acc.2] - Medida [op.acc.4] - Medida [op.exp.8]
O.Finalidad_10	Debe quedar reflejado quién accede a los datos en cada momento y qué acciones realiza sobre ellos: • La creación debe registrar fecha y hora y usuario que realiza el cambio • En modificación debe registrar quién realiza el cambio y registrar el dato antiguo y el dato nuevo • En la eliminación se debe reflejar qué dato se elimina • En el acceso, indicar el índice del dato accedido, usuario y fecha y hora • La vigencia de la tabla de auditoría puede ser la misma que la de los datos.	- Medida [op.acc.1] - Medida [op.acc.2] - Medida [op.acc.4] - Medida [op.exp.8]

3.1.2 OBJETIVO (2): ARQUITECTURA

Concepto	Descripción	RD 3/2010 (ENS)
O.Arq_1	La seguridad **DEBE** ser una parte integral del desarrollo del software y del ciclo de vida de la aplicación y su *backend*[18].	- Art. 39 - Medida [op.exp.11] - Medida [mp.sw.1]
O.Arq_2	Durante la fase de diseño de la aplicación, **DEBE** tenerse en cuenta que la aplicación y su *backend*, tratarán datos sensibles (categorías especiales de datos). Para lograr esto, la arquitectura de la aplicación **DEBE** controlar la recolección, el procesamiento, el almacenamiento	(Ver medidas del Objetivo (1): Finalidad de la aplicación.)

[18] Ver *iOS Security Framework* (Apple) y *Security for Android Developers* (Google).

	y la eliminación segura de los datos sensibles, a lo largo de su ciclo de vida.	
O.Arq_3	El ciclo de vida del material criptográfico **DEBE** ajustarse a una política que incluya elementos tales como la fuente de números aleatorios, información detallada sobre la segregación de las funciones de las claves, el periodo de validez de las claves de los certificados, el aseguramiento de la integridad mediante algoritmos hash, etc. La política **DEBERÍA** basarse en normas reconocidas[19].	- Medida [org.4] - Medida [op.acc.5] - Medida [op.exp.11] - Medida [mp.com.2] - Medida [mp.si.2] - Instrucción Técnica de seguridad de Criptología de empleo en el Esquema Nacional de Seguridad.
O.Arq_4	Si la aplicación utiliza un *backend* en la nube, el sistema de información en la nube **DEBE** ser conforme con el ENS[20] o poseer una certificación de seguridad para servicios en la nube[21].	- Medidas [op.ext], en relación con el resto de medidas del ENS que resulten de aplicación al sistema en nube. Observancia de las Guías: - CCN-STIC 823 Utilización de servicios en la nube. - CCN-STIC 811 Interconexión en el ENS. - CCN-STIC 812 Seguridad en entornos y aplicaciones web. - CCN-STIC 836 seguridad en VPN.
O.Arq_5	Las copias de seguridad y las copias de seguridad del sistema en la nube (*backend*) controladas por el	- Medida [mp.info.1] - Medida [mp.info.9]

[19] Tales como NIST: "Recommendation for Key Management", Revision 4 y BSI TR-02102 Cryptographic Mechanisms.
[20] En la categoría de seguridad Básica, Media o Alta, dependiendo del resultado del Análisis de Riesgos
[21] Por ejemplo, tal como el *Cloud Computing Compliance Controls Catalogue (C5)-Criteria to assess the information security of cloud services*, de la BSI.

	sistema operativo **NO DEBEN** contener datos sensibles que no estén cifrados.	
O.Arq_6	Las funciones de seguridad **DEBEN** implementarse siempre, tanto en la aplicación como en el *backend*, así como en todas las interfaces externas y los puntos finales de las API.	- Art. 18. - Art. 19. - Art. 20. - Art. 22. - Art. 39. - Medidas [mp.com] - Medida [mp.sw.1]
O.Arq_7	La aplicación **DEBE** proteger la autenticidad e integridad de la aplicación y su configuración. La aplicación **DEBERÍA** realizar regularmente una autocomprobación de la autenticidad e integridad del binario de la aplicación mediante una forma firma electrónica basada en un certificado.	- Art. 1.2. - Art. 19. - Art. 20. - Medida [org.3] - Medida [op.exp.2] - Medida [mp.com.3] - Medida [mp.info.4] Observancia de las Guías: - CCN-STIC 823 Utilización de servicios en la nube. - CCN-STIC 811 Interconexión en el ENS. - CCN-STIC 812 Seguridad en entornos y aplicaciones web. - CCN-STIC 836 seguridad en VPN.
O.Arq_8	Si la aplicación utiliza *frameworks* o librerías de terceros (por ejemplo, para la serialización de objetos), el fabricante **DEBE** informar claramente al usuario sobre el ámbito de su uso y el alcance de los mecanismos de seguridad utilizados. La aplicación **DEBE** garantizar el uso seguro de estas funciones. La aplicación **DEBE** garantizar que las funciones no utilizadas no puedan	- Art. 16. - Art. 18. - Art. 39. - Medida [op.pl.3] - Medida [op.pl.5] - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.s.2] - Medida [mp.s.8]

	ser activadas por terceros.	Observancia de las Guías: - CCN-STIC 823 Utilización de servicios en la nube. - CCN-STIC 811 Interconexión en el ENS. - CCN-STIC 812 Seguridad en entornos y aplicaciones web. - CCN-STIC 834 Protección frente a código dañino. - CCN-STIC 836 seguridad en VPN.
O.Arq_9	El código interpretado[22] que puede interactuar con las entradas del usuario (Webviews con JavaScript), **NO DEBE** tener acceso a la memoria cifrada o a los datos del usuario, excepto cuando sea estrictamente necesario para cumplir la finalidad de la aplicación.	- Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.s.2]
O.Arq_10	El fabricante **DEBE** proporcionar al usuario un medio sencillo y eficaz para notificar incidentes o problemas de seguridad.	- Art. 7. - Art. 15. - Art. 24. - Art. 36. - Art. 37. - Medida [op.exp.3] - Medida [op.exp.7] - Medida [op.exp.9] - Medida [op.ext.2] - Medida [op.mon.2] - Medida [mp.com.3] Observancia de las Guías: - CCN-STIC 817 Gestión

[22] Esto no incluye el código de los lenguajes de programación específicos de la plataforma (como Java o Kotlin para Android).

		de ciberincidentes.
O.Arq_11	El *backend* **DEBERÍA** ser capaz de forzar las actualizaciones relevantes para la seguridad de la aplicación.	- Art. 20. - Art. 26. - Medida [op.pl.2] - Medida [op.exp.4] Observancia de las Guías: - CCN-STIC 823 Utilización de servicios en la nube. - CCN-STIC 811 Interconexión en el ENS. - CCN-STIC 812 Seguridad en entornos y aplicaciones web. - CCN-STIC 836 seguridad en VPN.
O.Arq_12	El fabricante **PUEDE** proporcionar la aplicación y las actualizaciones a través de un canal de confianza en su propia tienda de aplicaciones.	- Art. 18. - Art. 21. - Art. 22. - Art. 33. - Medida [op.pl.2] - Medida [op.acc.7] - Medida [mp.com.3] Observancia de las Guías: - CCN-STIC 823 Utilización de servicios en la nube. - CCN-STIC 811 Interconexión en el ENS. - CCN-STIC 812 Seguridad en entornos y aplicaciones web. - CCN-STIC 836 seguridad en VPN.
O.Arq_13	Si la aplicación y las actualizaciones no se importan desde los	- Art. 21. - Medida [org.4]

	mecanismos habituales de la tienda de aplicaciones de la plataforma de hardware, **DEBEN** ser cifradas y firmadas usando medios criptográficos.	- Medida [op.acc.7] - Medida [op.exp.11] - Medida [mp.com.2] - Medida [mp.si.2] - Medida [mp.info.4] Observancia de las Guías: - CCN-STIC 807 Criptología de empleo en el ENS. - CCN-STIC 834 Protección frente a código dañino. - CCN-STIC 836 seguridad en VPN.
	El acceso a la base de datos (sistema de almacenamiento) se realiza siempre mediante mecanismo para evitar los ataques a base de datos y sus propios datos. No se permite el uso de consultas directas desde la aplicación a la base de datos.	-
	Se debe estructurar la aplicación con roles y comprobar que cada rol accede únicamente a su espacio de datos. Y cada usuario accede a sus datos.	- Medida [op.acc.1] - Medida [op.acc.2]
	Todo dato de entrada recibido por el usuario debe ser filtrado mediante librerías para evitar los ataques de inyección de código.	
	Los datos para aumentar su nivel de seguridad de acceso deben tener indicado qué usuarios pueden acceder a ellos. Dependiendo del caso funcional, se puede cambiar el usuario por un rol.	- Medida [op.acc.1] - Medida [op.acc.2]
	Se debe comprobar funcionalmente que cada usuario únicamente accede	- Medida [op.acc.1] - Medida [op.acc.4]

	a sus datos. En todas las pruebas funcionales se debe comprobar si un usuario puede acceder a datos de otros usuarios.	- Medida [op.acc.5]
	Toda comunicación con un sistema externo debe ir cifrada, para evitar los ataques Man In The Middle (MITM).	- Medida [op.acc.7] - Medida [mp.info.3]
	En la medida de lo posible se debe utilizar mecanismo de doble factor para acceder a la aplicación.	- Medida [op.acc.5]
	Se debe revisar el sistema de reinicio de contraseñas para evitar acceso indebido o reiniciarla sin las suficientes garantías de autenticidad del usuario.	- Medida [op.exp.2] - Medida [op.acc.1] - Medida [op.acc.6]

3.1.3 OBJETIVO (3): CÓDIGO FUENTE

Concepto	Descripción	RD 3/2010 (ENS)
O.Código_1	Las entradas de los usuarios **DEBEN** ser revisadas antes de su uso para descartar por completo la entrada de usuario que contenga valores dañinos.	- Medida [op.pl.2] - Medida [op.exp.2] - Medida [op.exp.3] - Medida [op.exp.6] - Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.info.1]
O.Código_2	El fabricante **DEBE** proporcionar datos estructurados con una sintaxis de escape.	- Medida [mp.sw.1] - Medida [mp.sw.2] -
O.Código_3	Los mensajes de error y las notificaciones **NO DEBEN** contener datos sensibles (como una credencial de usuario, por ejemplo).	- Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.info.1]
O.Código_4	Las posibles excepciones en el flujo del programa **DEBEN** ser interceptadas, gestionadas de manera controlada y documentadas.	- Medida [mp.sw.1] - Medida [mp.sw.2]
O.Código_5	En caso de excepciones en el flujo del programa con efectos críticos para la	- Medida [mp.sw.1] - Medida [mp.sw.2]

	seguridad, la aplicación **DEBERÍA** abortar el acceso a datos sensibles.	- Medida [mp.info.1]
O.Código_6	En aquellos los entornos con gestión manual de la memoria (es decir, la propia aplicación puede definir exactamente cuándo y dónde se lee o escribe de la memoria), la aplicación y la implementación del *backend* **DEBEN** utilizar funciones seguras alternativas (por ejemplo, *sprintf_s* en lugar de *printf*) para leer y escribir en los segmentos de memoria o incluso la posibilidad de usar variables con cifrado directo en memoria.	- Medida [mp.sw.1] - Medida [mp.sw.2]
O.Código_7	Todas las opciones de soporte al desarrollo (tales como llamadas de log, URL de desarrolladores, métodos de prueba, etc.) **DEBEN** eliminarse por completo del código de la versión de producción.	- Medida [mp.sw.2]
O.Código_8	El fabricante **DEBE** asegurarse de que no queden mecanismos de depuración en la versión de producción.	- Medida [mp.sw.2]
O.Código_9	La implementación de la aplicación **DEBERÍA** permitir mecanismos de seguridad de última generación en el entorno de desarrollo, tales como la minimización de código-byte y la protección de las pilas.	- Medida [mp.sw.1] - Medida [mp.sw.2]
[Source_10]	Toda introducción de datos por usuarios debe estar filtrada por librerías destinadas a ello, para evitar ataques de SQL o de introducción de datos javascript o html inadecuados.	
[Source_11]	No se deben realizar consultas directas a las bases de datos, se deben usar los mecanismos necesarios para tratar antes los datos (Ejemplo el uso de PreparedStatement).	
[Source_12]	Se debe tener en cuenta el uso de variables dinámicas, cuando se	

	terminen de usar todas deben ser apuntadas o redireccionadas a *null* para evitar ataques del tipo *use after free*.	

3.1.4 OBJETIVO (4): SOFTWARE DE TERCEROS

Concepto	Descripción	RD 3/2010 (ENS)
O.SwExt_1	Las librerías y *frameworks* de terceros **DEBEN** utilizar la última versión disponible para el sistema operativo de la plataforma en uso. Teniendo en cuenta posibles interacciones con otras librerías a la hora de elegir la versión.	- Art. 20. - Art. 26. - Medida [op.pl.2] - Medida [op.exp.4] - Medida [op.ext.1] - Medida [mp.sw.1] - Medida [mp.sw.2]
O.SwExt_2	El fabricante **DEBE** realizar comprobaciones periódicas en relación con las vulnerabilidades de las librerías y *frameworks* de terceros. Las funciones de las librerías y *frameworks* **NO DEBEN** utilizarse si se conoce alguna vulnerabilidad.	- Art. 20. - Art. 37. - Medida [op.pl.1] - Medida [op.pl.2] - Medida [op.exp.3] - Medida [op.ext.1] - Medida [op.sw.2]
O.SwExt_3	Las actualizaciones de seguridad para las librerías y *frameworks* **DEBEN** incorporarse sin demora. El fabricante **DEBE** poseer y comunicar una política de seguridad que determine el tiempo de uso tolerado de la aplicación y/o el *backend* en base a la criticidad de las vulnerabilidades explotables. Una vez superado dicho periodo de tiempo, la aplicación **DEBE** dejar de funcionar.	- Art. 20. - Art. 26. - Medida [org.1] - Medida [op.pl.2] - Medida [op.exp.4] - Medida [op.ext.1] - Medida [mp.sw.1] - Medida [mp.sw.2]
O.SwExt_4	El usuario **DEBE** ser informado sobre las medidas de mitigación que puede aplicar.	- Art. 7. - Art. 9. - Art. 13. - Medida [org.1] - Medida [op.exp.7] - Medida [op.ext.1] - Medida [mp.per.3] - Medida [mp.per.4]
O.SwExt_5	El fabricante **DEBE** verificar la confiabilidad de las librerías y	- Art. 20. - Art. 26.

	frameworks de terceros, antes de su uso.	- Art. 37. - Medida [op.pl.1] - Medida [op.pl.2] - Medida [op.exp.3] - Medida [op.ext.1] - Medida [mp.sw.1] - Medida [op.sw.2]
O.SwExt_6	La aplicación **NO DEBERÍA** compartir datos sensibles con software de terceros.	- Art. 21. - Medida [op.ext.1] - Medida [mp.info.1]
O.SwExt_7	Los datos recibidos a través de software de terceros **DEBERÍAN** ser validados. Nota / ejemplo: Excepciones a O.SwExt_6 y O.SwExt_7 son, por ejemplo, los *frameworks* y las librerías para el cifrado (TLS).	- Art. 21. - Medida [op.ext.1] - Medida [mp.com.2] - Medida [mp.com.3] - Medida [mp.info.1]
O.SwExt_8	El software de terceros que haya dejado de ser mantenido por el fabricante o el desarrollador, **NO DEBE** utilizarse.	- Art. 20. - Medida [op.pl.2] - Medida [op.exp.3] - Medida [op.ext.1] - Medida [op.sw.2]

3.1.5 OBJETIVO (5): IMPLEMENTACIÓN CRIPTOGRÁFICA

Concepto	Descripción	RD 3/2010 (ENS)
O.Cryp_1	Cuando la aplicación utiliza cifrado, **NO DEBEN** utilizarse claves *hard-coded*[23]. Esto no se aplicará a técnicas de vanguardia que ocultan de manera robusta la clave utilizada para ingeniería inversa (*Criptografía de caja blanca*). Si se utilizan claves estáticas, al menos una clave no estática **DEBE**	- Medida [org.4] - Medida [op.exp.11] - Medida [mp.si.2] - Medida [mp.sw.1] - Medida [mp.com.2] Observancia de la Guía: - CCN-STIC 807 Criptología de empleo

[23] El uso de *hard-coded keys* (también llamadas *claves integradas*) se refiere a la práctica de incrustar claves de cifrado en texto plano (no cifradas) y otros datos secretos (claves SSH, secretos de DevOps, etc.) en el código fuente, lo que ayuda a simplificar el desarrollo, pero, al mismo tiempo, plantea un considerable riesgo de seguridad.

	ser utilizada en el cifrado multicapa.	en el ENS.
O.Cryp_2	La aplicación **DEBE** utilizar implementaciones probadas para implementar primitivas criptográficas.	- Medida [org.4] - Medida [op.exp.11] - Medida [mp.si.2] - Medida [mp.sw.1] - Medida [mp.com.2] Observancia de la Guía: - CCN-STIC 807 Criptología de empleo en el ENS.
O.Cryp_3	La elección de las primitivas criptográficas **DEBE** ser apropiada para la aplicación y cumplir las especificaciones del estado de la técnica.	- Art. 20. - Medida [org.4] - Medida [op.exp.11] - Medida [mp.si.2] - Medida [mp.sw.1] - Medida [mp.com.2] Observancia de la Guía: - CCN-STIC 807 Criptología de empleo en el ENS.
O.Cryp_4	Las claves criptográficas **NO DEBEN** ser usadas para más de un propósito. Nota / ejemplo: Hay que distinguir entre el propósito de la protección mediante el cifrado y la autenticación. Se deben proporcionar claves diferentes para cada propósito.	- Medida [org.4] - Medida [op.exp.11] - Medida [mp.si.2] - Medida [mp.sw.1] - Medida [mp.com.2] Observancia de la Guía: - CCN-STIC 807 Criptología de empleo en el ENS.
O.Cryp_5	La robustez de las claves criptográficas **DEBE** estar alineada con el estado actual de la técnica.	- Art. 20. - Medida [org.4] - Medida [op.exp.11] - Medida [mp.si.2] - Medida [mp.sw.1] - Medida [mp.com.2] Observancia de la Guía: - CCN-STIC 807

		Criptología de empleo en el ENS.
O.Cryp_6	Todas las claves criptográficas **DEBERÍAN** estar ubicadas en un entorno resistente a la manipulación (como un entorno de ejecución seguro/de confianza integrado). Se considerarán las variantes para las diferentes plataformas de hardware.	- Medida [org.4] - Medida [op.exp.11] - Medida [mp.si.2] - Medida [mp.sw.1] - Medida [mp.com.2] Observancia de la Guía: - CCN-STIC 807 Criptología de empleo en el ENS.

3.1.5.1 NÚMEROS ALEATORIOS

Concepto	Descripción	RD 3/2010 (ENS)
O.Random_1	Todos los valores aleatorios empleados en operaciones de carácter sensible **DEBEN** ser generados usando un generador criptográfico de números aleatorios seguro.	No Determinado explícitamente en el ENS.
O.Random_2	La aplicación, en operaciones de carácter sensible, **DEBE** obtener números aleatorios de un generador de números aleatorios con alta entropía.	No Determinado explícitamente en el ENS.
O.Random_3	La aplicación DEBERÍA asignar al generador de números aleatorios una semilla compuesta por, al menos, tres parámetros de sistema independientes. No **DEBERÍA** ser posible determinar los parámetros desde fuera de la aplicación. Si la plataforma proporciona un hardware generador de números aleatorios que no permite la asignación de semillas, tal hardware generador de números aleatorios **PUEDE** ser utilizado en su lugar. Nota / ejemplo: Lo anterior	No Determinado explícitamente en el ENS.

	concierne a los generadores de números aleatorios tanto en el dispositivo de la aplicación como en el *backend*.	
O.Random_4	La aplicación **DEBERÍA** obtener un número aleatorio adecuado del *backend* para crear una semilla para el generador de números aleatorios. Nota / ejemplo: Antes de la primera conexión TLS, la aplicación introduce la entropía en el generador local de números aleatorios, según O.Random_3 (por ejemplo, a partir de la interacción con el usuario y los sensores del dispositivo), a través de una semilla. Establece una conexión inicial para obtener entropía adicional de la fuente de números aleatorios del *backend*. A continuación, la conexión se cierra inmediatamente. La aplicación tiene en cuenta la aleatoriedad obtenida, según O.Random_4, en el generador de números aleatorios local. Para la conexión TLS se utilizará en adelante la aleatoriedad de la fuente aleatoria local, que se ha aumentado con la entropía de la fuente de números aleatorios del *backend*.	No Determinado explícitamente en el ENS.

3.1.6 OBJETIVO (6): AUTENTICACIÓN

Concepto	Descripción	RD 3/2010 (ENS)
O.Auten_1	El fabricante **DEBE** documentar una política para la autenticación (de doble factor), la autorización (concepto de rol) y la terminación de una sesión de solicitud.	- Medida [org.3] - Medida [op.pl.2] - Medida [mp.acc.5] - Medida [op.acc.6] - Medida [mp.sw.1] - Medida [mp.s.2]

O.Auten_2	Para la conexión con un sistema de *backend*, la autenticación y autorización adecuadas **DEBEN** tener lugar en la interfaz del *backend*.	- Medida [org.3] - Medida [op.pl.2] - Medida [mp.acc.5] - Medida [op.acc.7] - Medida [mp.com.3] - Medida [mp.sw.1] - Medida [mp.s.2]
O.Auten_3	La aplicación **DEBERÍA** implementar separadamente los mecanismos de autenticación y las funciones de autorización. Si la aplicación requiere diferentes funciones, la autorización **DEBE** implementarse por separado para cada acceso a los datos.	- Medida [op.pl.2] - Medida [mp.acc.5] - Medida [op.acc.6] - Medida [op.acc.7] - Medida [mp.com.3] - Medida [mp.sw.1] - Medida [mp.s.2]
O.Auten_4	El usuario **DEBE** ser autenticado por un segundo factor antes de que se procesen los datos sensibles en la aplicación (autenticación escalonada).	- Medida [op.pl.2] - Medida [op.acc.5]
O.Auten_5	Para la autenticación del usuario en la sesión de la aplicación, el segundo factor **PUEDE** ser generado por el sistema de *backend*.	- Medida [op.pl.2] - Medida [mp.acc.5]
O.Auten_6	En la evaluación de un proceso de autenticación **DEBERÍA** incluirse información adicional (tal como el dispositivo utilizado, el nodo de acceso Wi-Fi utilizado o la hora del acceso). En caso de que se produzca una desviación de los parámetros previstos, **DEBE** adoptarse una medida de autenticación adicional (autenticación escalonada).	- Medida [op.pl.1] - Medida [op.pl.2] - Medida [mp.acc.5]
O.Auten_7	**DEBEN** existir políticas de contraseñas robustas para la autenticación basada en un nombre de usuario y una contraseña.	- Medida [org.2] - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 821 Normas de Seguridad - Apéndice V:

		Normas de creación y uso de contraseñas.
O.Auten_8	Para la autenticación basada en un nombre de usuario y una contraseña, la robustez de la contraseña utilizada **PUEDE** mostrarse al usuario. La información relativa a la robustez de la contraseña elegida **NO DEBE** conservarse en la memoria de la aplicación o en el *backend*.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 821 Normas de Seguridad - Apéndice V: Normas de creación y uso de contraseñas.
O.Auten_9	El usuario **DEBE** poder cambiar su contraseña. Esta operación **DEBE** requerir datos de autenticación de nuevo con el fin de no poder hacerlo mediante una sesión robada.	- Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 821 Normas de Seguridad - Apéndice V: Normas de creación y uso de contraseñas.
O.Auten_10	El *backend* y la aplicación **DEBEN** proporcionar medidas que impidan probar reiteradamente los parámetros de inicio de sesión (por ejemplo, las contraseñas). Esto puede lograrse, por ejemplo, retrasando los intentos posteriores de acceso o utilizando los llamados *captchas*.	- Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 821 Normas de Seguridad - Apéndice V: Normas de creación y uso de contraseñas.
O.Auten_11	Si la aplicación fue interrumpida (puesta en segundo plano), **DEBE** solicitarse una nueva autenticación.	- Medida [mp.eq.2]
	El procedimiento de recuperación de contraseña debe validarse para ser robusto en comprobar la autenticidad del usuario y no permita el robo del usuario por este mecanismo.	- Medida [op.pl.2] - Medida [op.exp.2] - Medida [op.acc.5]

3.1.6.1 AUTENTICACIÓN MEDIANTE BIOMETRÍA

Concepto	Descripción	RD 3/2010 (ENS)
O.Biom_1	El uso de sensores biométricos **NO DEBERÍA** ser utilizado como único mecanismo de autenticación. Sólo debería permitirse como parte de la autenticación de dos factores.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.
O.Biom_2	El fabricante **DEBE** definir la calidad y las características mínimas de un sensor biométrico para ser utilizado por la aplicación.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [org.3] - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.
O.Biom_3	La aplicación **DEBE** verificar el hardware del sensor biométrico contra una *lista negra* o *lista blanca* antes de su uso. El fabricante **DEBERÍA** mantener una lista blanca/negra de sensores biométricos	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria:

	seguros/inseguros. Una lista blanca/negra **DEBE** mantenerse disponible en el *backend*.	- Art. 20. - Medida [op.pl.2] - Medida [op.exp.3] - Medida [op.acc.5] - Medida [mp.sw.2] Observancia de la Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.
O.Biom_4	Antes de una autenticación mediante un sensor biométrico, la aplicación **DEBE** asegurarse siempre de que el hardware disponible cumple los requisitos especificados.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [org.3] - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.
O.Biom_5	Antes de que la aplicación utilice un sensor biométrico, **DEBE** asegurarse de que el sensor tiene las características biométricas de referencia del usuario del dispositivo para su comparación.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 140

		Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.
O.Biom_6	La aplicación **DEBE** determinar cuándo se han modificado los rasgos biométricos de referencia y denegar la inscripción si tales rasgos se modificaron posteriormente (es decir, desde la activación del mecanismo de control de la autenticación en la aplicación).	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.
O.Biom_7	La aplicación **DEBE** hacer uso de las funciones propias del sistema operativo (por ejemplo, desbloqueo de *KeyChain/KeyStore*) para evaluar la autenticación biométrica.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.pl.2] - Medida [op.acc.5] Observancia de la Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC - Anexo A.2: Dispositivos biométricos.

3.1.6.2 MEDIDAS DE AUTENTICACIÓN *STATEFUL* (CONDICIONADAS)[24]

Concepto	Descripción	RD 3/2010 (ENS)
O.AutSF_1	La gestión de las sesiones **DEBERÍA** realizarse mediante marcos seguros (véase O.Red_3).	No Determinado explícitamente en el ENS.
O.AutSF_2	Los identificadores de sesión **DEBEN** ser creados por el generador de números aleatorios del *backend*.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*]
O.AutSF_3	Los identificadores de sesión **DEBEN** protegerse como datos sensibles.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*]
O.AutSF_4	Los identificadores de sesión **NO DEBEN** almacenarse sin cifrar en medios de almacenamiento permanentes.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 21. - Medida [mp.eq.3]
O.AutSF_5	La aplicación **DEBE** finalizar la sesión de la aplicación después de un tiempo límite de sesión apropiado, según las recomendaciones de las mejores prácticas.	- Medida [mp.eq.2]
O.AutSF_6	Cuando finaliza una sesión de la aplicación, ésta **DEBE** borrar de forma	No Determinado explícitamente en el

[24] *Stateful Authentication*: Después de una autenticación con éxito, la aplicación genera un token aleatorio para enviar al usuario y crea en memoria o en una base de datos interna una sesión autenticada del usuario. Cuando un usuario intenta acceder a la aplicación con un determinado token, la aplicación intenta recuperar los datos de la sesión de la memoria, comprueba si la sesión es válida y decide si el usuario tiene acceso al recurso deseado o no.

	segura el identificador de la sesión, tanto en el dispositivo como en el *backend*.	ENS. Aplicación por defecto o complementaria: - Medida [op.acc.6]

3.1.6.3 MEDIDAS DE AUTENTICACIÓN *STATELESS* (NO CONDICIONADAS)[25]

Concepto	Descripción	RD 3/2010 (ENS)
O.Tokn_1	El *token* de autenticación **DEBERÍA** estar situado en una zona segura de la memoria del dispositivo terminal (por ejemplo, *KeyChain/KeyStore*). El token de autenticación **DEBE** estar protegido en el dispositivo contra un fácil acceso de terceros (por ejemplo, en el caso dispositivos rooted/jailbroken).	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*]
O.Tokn_2	**NO DEBEN** incrustarse datos sensibles en un token de autenticación.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*] - Medida [mp.info.1]
O.Tokn_3	Un token de autenticación **DEBE** incluir el nombre completo del *backend* y la solicitud **DEBE** verificar el nombre completo.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*]
O.Tokn_4	El *backend* **DEBE** utilizar un procedimiento adecuado para firmar	No Determinado explícitamente en el ENS.

[25] *Stateless Authentication*: Después de una autenticación con éxito, la aplicación genera un token con todos los datos necesarios, lo firma con una clave pública y lo envía de vuelta al usuario. Hay un estándar para la generación de tokens, es el JWT (JSON Web Token). El proceso está descrito en la especificación *OpenID Connect* (OIDC). Cuando un usuario intenta acceder a la aplicación con un token, la aplicación verifica la firma del token con una clave privada, comprueba si el token ha caducado, recupera todos los datos de la sesión del token y toma una decisión sobre si el usuario tiene acceso al recurso deseado o no.

	el token de autenticación.	Aplicación por defecto o complementaria: - Medidas [op.acc.*] - Medida [mp.info.4]
O.Tokn_5	La clave privada utilizada para firmar el token de autenticación **NO DEBE** estar presente ni almacenarse en el dispositivo.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*] - Medida [mp.info.4]
O.Tokn_6	El *backend* **DEBE** comprobar el token. El algoritmo de firma **NO DEBE** ser "ninguna". Tampoco se recomienda que el tipo de firma sea "HS256", "HS384" o "HS512", puesto que puede llevar a que el *backend* emplee la clave pública como clave privada si no está debidamente configurado, al ser un algoritmo de firma simétrico.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*] - Medida [mp.info.4]
O.Tokn_7	El *backend* **DEBE** rechazar la solicitud hecha con un token de autenticación inválido o sin firmar.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc.*] - Medida [mp.info.4]
O.Tokn_8	El *backend* **DEBE** tener en cuenta el periodo de vigencia cuando se evalúa la validez de un token.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc] - Medida [mp.info.4]
O.Tokn_9	El *backend* **DEBE** proporcionar al usuario los *tokens* de autenticación existentes cuando se le soliciten.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc]

		- Medida [mp.info.4]
O.Tokn_10	El *backend* **DEBE** permitir al usuario invalidar uno o todos los tokens de autenticación emitidos previamente (por ejemplo, en caso de pérdida o robo del dispositivo).	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medidas [op.acc]

3.1.7 OBJETIVO (7): ALMACENAMIENTO Y PROTECCIÓN DE DATOS

Concepto	Descripción	RD 3/2010 (ENS)
O.PD_1	La configuración de fábrica de la aplicación **DEBE** proporcionar la máxima protección y seguridad de los datos.	- Art. 16. - Art. 19. - Art. 21. - Medida [op.exp.2] - Medida [op.exp.3]
O.PD_2	Todos los datos sensibles **DEBEN** ser almacenados de forma cifrada. Esto se aplica tanto al almacenamiento volátil (por ejemplo, en la memoria de trabajo) como al almacenamiento permanente (por ejemplo, en un entorno en la nube), incluyendo las claves criptográficas, con excepción del cifrado de la memoria. Se **DEBERÍA** dar preferencia a una gestión de claves de la plataforma soportada por hardware. Si la plataforma garantiza una protección suficiente de las claves (por ejemplo, en el entorno integrado de ejecución seguro/de confianza, la aplicación **PUEDE** almacenar las claves en texto plano.	- Art. 21. - Medida [op.exp.11] - Medida [mp.eq.3] - Medida [mp.si.2] - Medida [mp.info.1] - Medida [mp.info.3]
O.PD_3	Todos los datos sensibles **DEBERÍAN** almacenarse en un entorno protegido contra la visualización, el acceso y la manipulación (como el entorno integrado de ejecución seguro/de confianza). De esta manera, se	- Art. 21. - Medida [mp.eq.3] - Medida [mp.info.1]

	DEBERÍA alcanzar el mayor nivel posible de protección para la plataforma individual o el dispositivo final.	
O.PD_4	La aplicación **NO DEBE** poner a disposición de terceros ningún recurso que permita el acceso a datos sensibles.	- Art. 21. - Medida [op.acc.7] - Medida [mp.info.1]
O.Tokn_5	Todos los datos sensibles recopilados **NO DEBEN** guardarse en la aplicación o en su *backend* tras su uso. La aplicación **DEBE** respetar los principios de minimización de datos y de limitación de la finalidad[26].	- Art. 21. - Art. 27. - Medida [mp.info.1]
O.PD_6	Los datos sensibles **DEBEN** ser almacenados y procesados en el sistema de *backend*.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Art. 19. - Art. 21. - Art. 22. - Medida [op.acc.7] - Medida [op.exp.2] - Medida [mp.sw.1]
O.PD_7	Si se utilizan dispositivos de grabación (tales como cámaras, por ejemplo), **DEBEN** eliminarse todos los metadatos con relevancia para la protección de datos, tales como las coordenadas GPS del lugar de grabación, el hardware utilizado, etc.	- Art. 27. - Medida [mp.info.1]
O.PD_8	Cuando se recaben datos sensibles **DEBE** evitarse el uso de dispositivos de grabación (una cámara, por ejemplo), puesto que otras aplicaciones podrían acceder a esos datos (a través de una galería de	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria:

[26] Ambos principios, recogidos en el RGPD.

	imágenes, por ejemplo).	- Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_9	Cuando se introducen datos sensibles a través del teclado, la aplicación **DEBERÍA** evitar que los datos puedan ser visibles por terceros, contemplando específicamente las cachés, los procedimientos de autocorrección y autocompletado, dispositivos de entrada de terceros y cualquier forma de almacenamiento que pueda ser analizado por terceros.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_10	Cuando se introducen datos sensibles, su almacenamiento temporal en el portapapeles **DEBERÍA** desactivarse. La aplicación, sin embargo, **PUEDE** implementar su propio portapapeles, que estará protegido contra el acceso de otras aplicaciones.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_11	Los datos sensibles, como los datos biométricos o las claves privadas, **NO DEBEN** exportarse desde el componente en el que se generaron.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_12	Cuando se muestren datos sensibles, la aplicación **DEBERÍA** impedir el acceso de terceros y el almacenamiento de los contenidos de la pantalla (por ejemplo, las capturas de pantalla y las pantallas para el	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria:

	cambio de aplicación).	- Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_13	La aplicación **NO DEBE** escribir datos sensibles en ficheros de log u otros mensajes o notificaciones que no hayan sido expresamente habilitados por el usuario (véase O.Plat_4).	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_14	La aplicación **DEBE** asegurarse de que todos los datos sensibles se cifren cuando el dispositivo se bloquee. Nota/ejemplo: Las versiones de plataformas más antiguas permiten parcialmente el almacenamiento de la aplicación en medios de almacenamiento externos que no están sujetos al cifrado de almacenamiento. Esto **DEBE** estar prohibido.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1] - Medida [mp.info.3]
O.PD_15	La aplicación **DEBE** proporcionar los datos almacenados localmente mediante una conexión segura del dispositivo.	- Art. 22. - Medida [op.pl.2] - Medida [mp.eq.3]
O.PD_16	Si la plataforma no protege contra el robo del medio de almacenamiento seleccionado (por ejemplo, usando tarjetas SD sin cifrar), la aplicación **DEBE** informar al usuario del riesgo cuando se seleccione el medio de almacenamiento en cuestión. Nota / ejemplo: El cifrado de los datos a nivel de aplicación debe mantenerse en todo caso.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1] - Medida [mp.info.3]

O.PD_17	La aplicación **DEBE** garantizar que todos los datos sensibles y la información específica de inicio de sesión almacenados en el dispositivo se eliminen completamente cuando se desinstale la aplicación.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 19. - Art. 21. - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_18	La aplicación **DEBE** proporcionar al usuario la opción de que todos los datos sensibles y la información específica para el acceso a la aplicación también se eliminen completamente en el *backend* cuando se desinstale la aplicación. Si el usuario decide no borrar los datos en el *backend*, **DEBE** definirse un período máximo de retención. El usuario **DEBE** ser informado sobre la duración del período de retención. Después de que este periodo haya expirado, todos los datos sensibles y la información específica de inicio de sesión de la aplicación **DEBEN** ser eliminados completamente. El usuario **DEBE** tener la oportunidad de borrar por completo todos los datos, incluso antes de que finalice el período de retención. Nota / ejemplo: Permitir la por cambio de dispositivo, sin pérdida del historial.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 19. - Art. 21. - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.info.1]
O.PD_19	Para contrarrestar un posible mal uso de los datos tras la pérdida de un dispositivo, la aplicación **PUEDE** implementar un “kill switch”, es decir, una sobre-escritura intencionada y	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria:

	segura de los datos del usuario en el dispositivo a nivel de aplicación, activada por el *backend*. El fabricante **DEBE** implementar a través del *backend* mecanismos de autenticación fuertes para prevenir la activación no intencionada del "kill switch" por parte del usuario.	- Art. 19. - Art. 21. - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1]

3.1.8 OBJETIVO (8): RECURSOS DE PAGO

Concepto	Descripción	RD 3/2010 (ENS)
O.Pago_1	La solicitud de la aplicación **DEBE** indicar al usuario qué servicios están sujetos a costes adicionales.	No Determinado explícitamente en el ENS.
O.Pago_2	La aplicación **DEBE** obtener el consentimiento del usuario antes de llevar a cabo cualquier acción que esté sujeta a un cargo.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [op.exp.2] - Medida [mp.info.1]
O.Pago_3	La aplicación **DEBE** obtener el consentimiento del usuario antes de solicitar el acceso (por ejemplo, permisos de Android) a los recursos de pago. Nota / ejemplo: El envío de SMS puede comportar costes y, por lo tanto, debe requerir consentimiento.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [op.exp.2] - Medida [mp.info.1]
O.Pago_4	La aplicación **PUEDE** obtener el consentimiento permanente del usuario para acceder a recursos de pago de uso frecuente, en la medida en que esto sea apropiado para la finalidad de la aplicación.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16.

		- Medida [op.exp.2] - Medida [mp.info.1]
O.Pago_5	La aplicación **DEBE** permitir al usuario retirar el consentimiento previamente otorgado.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [op.exp.2] - Medida [mp.info.1]
O.Pago_6	La aplicación **DEBERÍA** almacenar en el *backend* el histórico de todos los pagos hechos. El histórico de transacciones, incluyendo los metadatos, **DEBEN** ser tratados como datos sensibles según [O.Finalidad_8].	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [op.exp.2] - Medida [mp.info.1]
O.Pago_7	Si la aplicación ofrece funciones de pago, el fabricante **DEBE** implementar una política que impida a terceros rastrear los flujos de pago por el uso de las funciones de la aplicación. Nota/ejemplo: El procesamiento de pagos periódicos es un método posible para ocultar a terceros la intensidad y frecuencia real del uso.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [org.1] - Medida [op.exp.2] - Medida [mp.info.1]
O.Pago_8	La aplicación **DEBE** ofrecer al usuario una visión general de los costes incurridos. Si los costes son debidos a accesos individuales, la aplicación **DEBE** mostrar una visión general de los accesos.	No Determinado explícitamente en el ENS.
O.Pago_9	La validación de las transacciones de pago **DEBE** llevarse a cabo en el *backend*.	No Determinado explícitamente en el ENS.

O.Pago_10	Los procedimientos de pago de terceros **DEBEN** cumplir los requisitos del software de terceros (véase el epígrafe 3.1.4).	No Determinado explícitamente en el ENS.

3.1.9 OBJETIVO (9): COMUNICACIÓN DE RED

Concepto	Descripción	RD 3/2010 (ENS)
O.Red_1	Toda la comunicación de la aplicación a través de la red **DEBE** estar cifrada con TLS en todo momento.	- Art. 21. - Art. 22. - Medida [mp.com.3] - Medida [mp.info.3] - Medida [mp.s.2]
O.Red_2	La configuración de las conexiones TLS **DEBE** ser de última generación y seguir las recomendaciones de las mejores prácticas actuales[27].	- Art. 21. - Art. 22. - Medida [mp.com.3] - Medida [mp.info.3] - Medida [mp.s.2]
O.Red_3	Para establecer canales seguros, la aplicación **DEBE** utilizar la funcionalidad de seguridad de la plataforma del sistema operativo o *frameworks* o librerías verificados en materia de seguridad.	- Art. 20. - Art. 21. - Art. 22. - Medida [op.pl.2] - Medida [op.exp.4] - Medida [mp.eq.3] - Medida [mp.com.3] - Medida [mp.info.3] - Medida [mp.s.2]
O.Red_4	La solicitud **DEBE** sustentarse en una jerarquía adecuada de certificados, es decir, **NO DEBE** aceptar certificados cuya cadena de confianza no se considere segura por el fabricante[28].	- Art. 33. - Medida [op.pl.2] - Medida [op.acc.5] - Medida [op.exp.4] - Medida [mp.info.4] - Medida [mp.s.2]
O.Red_5	La aplicación **DEBE** comprobar el certificado del servidor del *backend*.	- Art. 33. - Medida [op.pl.2]

[27] Véase, por ejemplo: BSI: Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths - Part 2 – Use of Transport Layer Security (TLS)

[28] Ver: C. Evans, C. Palmer, R. Sleevi, Google Inc., "Public Key Pinning Extension for HTTP", versión de abril de 2015, disponible en: https://tools.ietf.org/html/rfc7469

		- Medida [op.acc.5] - Medida [op.exp.4] - Medida [mp.info.4] - Medida [mp.s.2]
O.Red_6	El *backend* **DEBE** rechazar las conexiones cuya versión de protocolo o suite de cifrado no cumpla con la normativa de aplicación[29].	- Art. 21. - Art. 22 - Medida [mp.com.3] - Medida [mp.info.3] - Medida [mp.s.2]
O.Red_7	La aplicación **DEBE** validar la integridad de las respuestas del *backend*.	- Medida [mp.com.3] - Medida [mp.s.2]
O.Red_8	La aplicación **DEBE** deshabilitar los mecanismos de retroceso específicos de la plataforma (por ejemplo, la exclusión voluntaria del tráfico de texto en claro).	No Determinado explícitamente en el ENS.
O.Red_9	La aplicación **DEBERÍA** mantener archivos de logs en el *backend* para todas las conexiones establecidas. Cuando se utilicen servidores proxy intermedios, **DEBE** asegurarse que las cabeceras HTTP se capturen completamente (por ejemplo, X-*forwarded-for*).	- Art. 14. - Art. 23. - Medida [op.exp.8] - Medida [op.exp.10]
O.Red_10	Un inicio abortado **DEBE** ser registrado como un evento de seguridad en el *backend*.	- Medida [op.exp.7] - Medida [op.exp.8] - Medida [op.exp.9] - Medida [op.exp.10]

3.1.10 OBJETIVO (10): INTERACCIONES ESPECÍFICAS DE LA PLATAFORMA

Concepto	Descripción	RD 3/2010 (ENS)
O.Plat_1	Para usar la aplicación, el dispositivo terminal **DEBE** tener protección de dispositivo (contraseña, bloqueo de patrón, etc.). El fabricante **DEBE**	- Art. 16. - Art. 19. - Art. 21. - Medida [op.pl.2]

[29] Por ejemplo: BSI: Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths - Part 2 – Use of Transport Layer Security (TLS)

	informar al usuario de las consecuencias de no tener activada la protección.	- Medida [op.acc.5] - Medida [op.acc.6] - Medida [op.exp.2] - Medida [mp.eq.2]
O.Plat_2	La aplicación **NO DEBE** solicitar ningún permiso que no sea el necesario para cumplir con su finalidad principal.	- Art. 16. - Medida [op.pl.2] - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.info.1]
O.Plat_3	La aplicación **DEBE** informar al usuario del propósito de los permisos que se solicitan y de las consecuencias si el usuario no los concede.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [op.pl.2] - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.info.1]
O.Plat_4	La aplicación **PUEDE** proporcionar al usuario opciones para mostrar mensajes y notificaciones, incluidas las de contenido sensible, si procede. Por defecto, **DEBE** estar desactivado.	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Art. 16. - Medida [op.pl.2] - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.sw.2] - Medida [mp.info.1]
O.Plat_5	La aplicación **DEBERÍA** restringir el acceso a las rutas de archivo que se designen.	No Determinado explícitamente en el ENS. Aplicación por defecto o

	Nota / ejemplo: Por ejemplo, haciendo una lista blanca de rutas de archivos.	complementaria: - Art. 16. - Medida [op.pl.2] - Medida [op.exp.2] - Medida [op.exp.3] - Medida [mp.sw.1] - Medida [mp.sw.2]
O.Plat_6	La aplicación **DEBE** implementar restricciones de acceso a todos los datos.	- Art. 16. - Art. 19. - Medida [op.pl.2] - Medidas [op.acc.*]
O.Plat_7	La aplicación **DEBE** restringir los mensajes de difusión solo a las aplicaciones autorizadas.	- Art. 16. - Art. 19. - Medida [op.pl.2] - Medidas [op.acc.*]
O.Plat_8	La aplicación **NO DEBE** enviar ningún dato sensible en los mensajes de difusión.	- Art. 16. - Art. 19. - Medida [op.pl.2] - Medida [mp.info.1]
O.Plat_9	**DEBERÍA** evitarse el ofrecimiento de funcionalidades sensibles a través de comunicaciones entre procesos. Si el ofrecimiento es necesario para cumplir la finalidad, las funcionalidades ofrecidas **DEBEN** protegerse adecuadamente.	- Art. 16. - Medida [op.exp.2] - Medida [op.exp.3] - Medida [op.sw.1]
O.Plat_10	La aplicación **DEBERÍA** evitar que JavaScript esté activo mientras se usa WebView. Si JavaScript es indispensable para la aplicación, la aplicación DEBE rechazar JavaScript de fuentes ajenas al control del fabricante.	- Art. 20. - Medida [op.exp.1] - Medida [op.exp.4] - Medida [op.sw.1]
O.Plat_11	Si la aplicación cambia a segundo plano, **DEBE** eliminar todos los datos sensibles de la vista actual (Vistas en iOS y Actividades en Android).	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [mp.info.1]

O.Plat_12	La aplicación **DEBE** deshabilitar cualquier manejador de protocolos que no se necesite en WebViews.	- Art. 16. - Art. 19. - Medida [op.exp.2] - Medida [op.exp.3] - Medida [op.sw.1]
O.Plat_13	La aplicación **DEBE** eliminar las cookies específicas de la aplicación después de salir de la misma.	- Medida [op.exp.2] - Medida [op.exp.3] - Medida [op.sw.1] - Medida [mp.info.1]
O.Plat_14	Al finalizar, la aplicación **DEBERÍA** sobrescribir de forma segura todos los datos específicos del usuario en la memoria de trabajo.	- Medida [op.exp.2] - Medida [op.exp.3] - Medida [op.sw.1] - Medida [mp.info.1]

3.1.11 OBJETIVO (11): RESILIENCIA

Concepto	Descripción	RD 3/2010 (ENS)
O.Resi_1	La aplicación **DEBE** proporcionar al usuario recomendaciones accesibles de mejores prácticas para el uso seguro de la aplicación y su configuración.	- Medida [org.2] - Medida [org.3] - Medida [mp.sw.1]
O.Resi_2	La aplicación **DEBE** detectar los dispositivos *rooted* o *jailbroken* de acuerdo con el estado actual de la técnica y responder adecuadamente. El fabricante **DEBE** señalar los riesgos para los datos del usuario si se continúa con la aplicación (por ejemplo, que los datos puedan ser revelados). Otra respuesta apropiada sería dar por terminada la aplicación.	- Medida [org.2] - Medida [mp.sw.1] - Medida [mp.info.1]
O.Resi_3	La aplicación **DEBE** detectar y prevenir de forma fiable el inicio en un entorno de desarrollo/depuración.	- Medida [op.acc.3] - Medida [mp.sw.1] - Medida [mp.sw.2]
O.Resi_4	La aplicación **DEBE** abortar su inicio si se inicia con derechos de usuario inusuales (por ejemplo, *root* o "*nadie*").	No Determinado explícitamente en el ENS.

		Aplicación por defecto o complementaria: - Medida [mp.sw.1]
O.Resi_5	La aplicación **DEBE** verificar la integridad del dispositivo antes de procesar datos sensibles (como Google Safety.Net).	- Medida [mp.com.3] - Medida [op.info.1] - Medida [mp.sw.1]
O.Resi_6	La aplicación **DEBE** verificar la integridad del *backend* antes de acceder a él (véase también O.Red_4).	- Art. 33. - Medida [op.pl.2] - Medida [mp.s.2]
O.Resi_7	La aplicación **DEBE** implementar medidas de *hardening*, tales como comprobación de la integridad, antes de cada procesamiento de datos sensibles dentro del flujo del programa.	- Art. 20. - Medida [mp.com.3]
O.Resi_8	La aplicación **DEBE** implementar medidas exigentes contra la ingeniería inversa y **PUEDE** utilizar medidas de ofuscación, tales como la ofuscación de código y el cifrado de cadenas (*strings*).	No Determinado explícitamente en el ENS. Aplicación por defecto o complementaria: - Medida [mp.sw.1]
O.Resi_9	La aplicación **DEBE** implementar mecanismos de control de acceso, teniendo en cuenta las diferentes plataformas y sus versiones, de manera que se evite el uso indebido de los recursos al cambiar la versión de la plataforma y se logre una protección suficiente de todos los activos en cada entorno de ejecución.	- Art. 16. - Medida [op.pl.2] - Medidas [op.acc.*] - Medida [mp.eq.3] - Medida [mp.s.2]