Instrucción técnica para la homologación del material de apuestas y verificación del cumplimiento de los requisitos técnicos aplicables a los medios informáticos.

Epoche and Espri S.L.
Edificion Veganova
Avenida de la Vega, 1,
28108, Alcobendas
Madrid, España
Tel. (+34) 91 490 29 00

Epoche and Espri Corporation
Fairfax Business Center
Legato Road, Suite 1100
Fairfax, 22033
Virginia, USA
Tel. (+1) 888-877-9506

PREÁMBULO. **4**
CAPÍTULO I. DE LOS REQUISITOS DE SEGURIDAD. **5**
ARTÍCULO 1. 5
ARTÍCULO 2. 5
DISPOSICIÓN ADICIONAL **6**
ANEJO I. PERFIL DE PROTECCIÓN DEL SISTEMA DE INFORMACIÓN **7**
REFERENCIAS **7**
DEFINICIONES **8**
ABREVIATURAS **8**
IDENTIFICACIÓN **9**
OBJETO DEL PERFIL DE PROTECCIÓN **9**
RESUMEN DEL STOE **9**
USO DEL STOE 10
TIPO DE STOE 11
INTERFACES CON OTROS SISTEMAS REQUERIDOS POR EL STOE 11
ORGANIZACIÓN DE DOMINIOS 12
DECLARACIÓN DE CONFORMIDAD CON RESPECTO A LA NORMA [ISO19791] Y [CC31P2] **16**
CONFORMIDAD DE OTROS PP **16**
DEFINICIÓN DEL PROBLEMA DE SEGURIDAD **17**
ACTIVOS DEL STOE 17
DEFINICIÓN DEL RIESGO 20
POLÍTICAS ORGANIZATIVAS 23
OBJETIVOS DE SEGURIDAD **25**
OBJETIVOS DE SEGURIDAD FUNCIONALES DEL STOE 25
OBJETIVOS DE SEGURIDAD FUNCIONALES DE SISTEMAS OPERACIONALES EXTERNOS 27
OBJETIVOS DE SEGURIDAD DE GARANTÍA DEL STOE 27
JUSTIFICACIÓN DE LOS OBJETIVOS DE SEGURIDAD 28
DEFINICIÓN DE COMPONENTES EXTENDIDOS **30**
REQUISITOS DE SEGURIDAD DEL STOE **31**
REQUISITOS QUE APLICAN A LOS TRES DOMINIOS **31**
REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL 31
AUDITORÍA 31
PROTECCIÓN DE DATOS 33
DOMINIO CLIENTES **36**
REQUISITOS FUNCIONALES TÉCNICOS 36
REQUISITOS DE IDENTIFICACIÓN Y AUTENTICACIÓN. 36
REQUISITOS DE PROTECCIÓN DE DATOS DE USUARIO 37
FUNCIONES DE GESTIÓN DE LA SEGURIDAD 38
COMUNICACIONES 39
PASARELAS DE PAGO 39
AUDITORÍA 40
REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL 41
DOMINIO OPERADORES INTERNOS **42**
REQUISITOS FUNCIONALES TÉCNICOS 42
REQUISITOS DE IDENTIFICACIÓN Y AUTENTICACIÓN. 42
REQUISITOS DE PROTECCIÓN DE DATOS DE USUARIO 42
FUNCIONES DE GESTIÓN DE LA SEGURIDAD 45
FUNCIONES CRIPTOGRÁFICAS 46

INTEGRIDAD, NO REPUDIO DE LAS APUESTAS Y BOLETOS 46
ESTABLECIMIENTO DE CRITERIOS DE ALEATORIEDAD EN AQUELLAS APUESTAS EN QUE ASÍ SE PRECISE 50
COMUNICACIONES 51
COMUNICACIONES CON LOS CLIENTES U OTRAS ENTIDADES EXTERNAS 51
COMUNICACIONES CON LAS MÁQUINAS DE APUESTAS 52
AUDITORÍA 52
REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL 53
DOMINIO SOPORTE 54
REQUISITOS FUNCIONALES TÉCNICOS 54
REQUISITOS DE IDENTIFICACIÓN Y AUTENTICACIÓN. 54
REQUISITOS DE PROTECCIÓN DE DATOS DE USUARIO. POLÍTICA DE CONTROL DE ACCESO 55
FUNCIONES DE GESTIÓN DE LA SEGURIDAD 57
TOLERANCIA A FALLOS Y RECUPERACIÓN 58
FUNCIONES CRIPTOGRÁFICAS 59
CIFRADO DE LOS DISCOS DE LOS SERVIDORES 59
CIFRADO DE LOS BACKUPS 60
BORRADO SEGURO DE BACKUPS 61
FUENTE DE TIEMPO 62
AUDITORÍA Y DETECCIÓN DE INTRUSOS 62
REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL 63
POLÍTICA DE SEGURIDAD 63
PERSONAL 66
GESTIÓN DE RIESGOS 69
GESTIÓN DE LOS ACTIVOS 69
GESTIÓN DE LA SEGURIDAD 70
GESTIÓN DE SISTEMAS TI 71
GESTIÓN DE ACTUALIZACIONES 71
POLÍTICA ANTI-MALWARE 73
COPIAS DE SEGURIDAD 74
REGISTRO Y NOTIFICACIÓN DE INCIDENCIAS DE SEGURIDAD 75
PLAN DE CONTINUIDAD DEL SERVICIO 75
INSTALACIONES Y EQUIPAMIENTO 77
REQUISITOS DE GARANTÍA DE SEGURIDAD 86
REQUISITOS DE GARANTÍA ASOCIADOS A LA EVALUACIÓN DE SST 86
REQUISITOS DE GARANTÍA ASOCIADOS A LA EVALUACIÓN DE STOE 87
DESARROLLO/ FASE DE INTEGRACIÓN 88
FASE DE INSTALACIÓN 88
FASE DE OPERACIÓN 89
FASE DE MODIFICACIÓN 90
JUSTIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD 91
CUMPLIMIENTO DEL REGLAMENTO DE APUESTAS DE LA CIUDAD DE CEUTA 91
JUSTIFICACIÓN DE LOS REQUISITOS FUNCIONALES DE SEGURIDAD 105
JUSTIFICACIÓN DE LOS REQUISITOS DE GARANTÍA DE SEGURIDAD 110
ANEJO II. AUDITORÍA DE LA SEGURIDAD. 113

Preámbulo.

Establece el Reglamento de Apuestas de la Ciudad de Ceuta, en su Artículo 23, los requisitos aplicables a los sistemas técnicos en el caso de apuestas que se formalicen por medios informáticos o electrónicos interactivos.

El Capítulo II del citado reglamento, en su Artículo 7, establece la necesidad de acreditar la solvencia técnica, en particular, la necesidad de disponer de unos medios informáticos seguros para la organización y comercialización de las apuestas que garanticen el correcto funcionamiento de las mismas, requiriendo en su Artículo 8 de un informe de auditoría que avale tal extremo.

En primer lugar, dada la complejidad de garantizar la seguridad de tales medios informáticos, se hace necesario desarrollar con mayor detalle técnico del indicado en el Reglamento de Apuestas de la Ciudad de Ceuta las características, funcionalidad y prestaciones que, en materia de seguridad y garantías a los usuarios de los servicios de apuestas autorizados por la Ciudad de Ceuta se deben prestar y mantener.

Adicionalmente, y dado que la certificación del cumplimiento de unos requisitos de seguridad determinados es función y competencia ya desarrolladas en la Administración General del Estado, en virtud de la ORDEN PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, resulta conveniente y aconsejable la remisión a la autoridad técnica y administrativa en estas cuestiones la cuestión del cumplimiento de los requisitos técnicos de seguridad exigibles a las personas jurídicas a las que la Ciudad de Ceuta pueda conceder la autorización de organización y comercialización de apuestas.

Esta instrucción técnica desarrolla, por tanto, los requisitos de seguridad exigibles a los sistemas informáticos regulados por el Reglamento de Apuestas de la Ciudad de Ceuta, sometiendo la certificación de su cumplimiento a la correspondiente resolución de certificación que el Centro Criptológico Nacional puede otorgar conforme a lo establecido en la ORDEN PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Capítulo I. De los requisitos de seguridad.

Artículo 1.

Los requisitos de seguridad detallados exigibles a los medios informáticos empleados en la organización y comercialización de las apuestas son los indicados en el Anejo I, "Perfil de Protección del Sistema de Información".

Tales requisitos de seguridad se expresan conforme a los formalismos y conceptos de la norma ISO/IEC 15408 "Common Criteria", ampliados en su aplicación a un sistema de apuestas informático por lo establecido en ISO/IEC TR 19791 "Information technology – Security techniques – Security assessment of operational systems".

Artículo 2.

A los efectos de lo indicado en los artículos 8, 9 y 49.5 del vigente Reglamento de Apuestas de la Ciudad de Ceuta, el único informe de auditoría que se admitirá como prueba de cumplimiento de los requisitos de seguridad indicados en el anterior artículo será el certificado de conformidad emitido por el Centro Criptológico Nacional, a instancias de la empresa autorizada, a través de la correspondiente publicación en el Boletín Oficial del Estado de la resolución estimatoria de certificación.

Disposición adicional

La exigencia de la certificación concedida por el Centro Criptológico Nacional entrará en vigor a los dos meses de la publicación de esta instrucción técnica en el Boletín Oficial de la Ciudad de Ceuta.

Hasta tal fecha, se admite como medio de acreditación de la conformidad de los requisitos de seguridad un informe de una empresa auditora, con personal acreditado en auditorías de seguridad informática, sobre la solvencia técnica del sistema informático previsto para la organización y comercialización de las apuestas, conforme al programa de auditoría detallado en el Anejo II.

Anejo I. Perfil de Protección del Sistema de Información

Referencias

[ISO19791]	ISO/IEC TR 19791 Information technology – Security techniques – Security assessment of operational systems
[CC31p2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components Version 3.1 R3 Jul 2009
[LOPD]	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
[RMS]	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.
[RACC]	REGLAMENTO DE APUESTAS DE LA CIUDAD DE CEUTA, B. O. C. CE. - 4.948 Martes 18 de Mayo de 2010
[RECSTI]	ORDEN PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Definiciones

1 Son de aplicación las definiciones incluidas en el REGLAMENTO DE APUESTAS DE LA CIUDAD DE CEUTA, B. O. C. CE. - 4.948 Martes 18 de Mayo de 2010.

2 **Sistema operacional:** sistema de información que incluye sus aspectos organizativos (no de las tecnologías de la información - TI), considerado en el contexto de su entorno de operacional. Incluye la combinación de procesos, procedimientos y personas, integrados con funciones y mecanismos de las TIs, aplicados juntos para establecer un nivel aceptable de riesgo residual en un entorno operacional definido.

3 **Dominio de seguridad**. Partes de un sistema operacional (subsistemas y componentes) que están bajo el mismo conjunto de políticas de seguridad.

Abreviaturas

CC	Common Criteria
IDS	Intrusion Detection System
I&A	Identificación y Autenticación
OSF	Operacional Security Function
SPP	System Protection Profile
SSA	System Security Assurance
SSF	System Security Functionality
SST	System Security Target
STOE	System Target of Evaluation
TOE	Target of Evaluation
TSF	TOE Security Functionality (*)

(*) En [CC31p2] el acrónimo TSF significa *TOE Security Functionality*. Sin embargo en [ISO19791], TSF hace referencia a *Technical Security Function*. A menos que se indique lo contrario, el significado de TSF será este último, tal y como se identifica en [ISO19791].

Identificación

Título	Perfil de Protección. Sistema de Formalización de Apuestas.
Versión	1.1
Fecha de Publicación	13 de septiembre de 2010
Autor	Ayuntamiento de la Ciudad Autónoma de Ceuta

4 Este documento es un **Perfil de Protección de Sistema** (SPP), en el que se especifican los requisitos de seguridad funcionales (técnicos y de control) y de garantía para un sistema de formalización de apuestas on-line, conforme a la norma [ISO19791].

Objeto del Perfil de Protección

5 Este perfil de protección contiene las exigencias que deben cumplir los sistemas informáticos e interactivos así como las medidas de seguridad y organización de las empresas solicitantes de autorización para la organización y comercialización de apuestas, entendidas éstas como la actividad por la que se arriesga una cantidad de dinero sobre los resultados de un acontecimiento o un juego previamente determinado, de desenlace incierto y que pueden ser ajenos a las partes intervinientes en dicha apuesta, o bien, dependientes de la habilidad de los apostantes en juego.

Resumen del STOE

6 El STOE proporciona una gestión integral de apuestas online sobre sucesos, cuya resolución final determinará un resultado concreto, hecho que sucede, por ejemplo, en eventos deportivos. En definitiva, el STOE actúa a modo de casa de apuestas, y para ello, distribuye la funcionalidad y su acceso en diferentes partes.

7 El sistema lleva a cabo una gestión de los mercados de eventos sobre los que se pueden realizar apuestas, junto con las tasas asociadas a cada resultado posible, de modo que presenta dicha información a los apostantes.

8 Cada apuesta realizada por un apostante queda debidamente registrada, y este registro emplea métodos que garantizan la integridad de la apuesta, así como el no repudio por parte del apostante. El recuento total de apuestas y la gestión monetaria asociado a las mismas se lleva a cabo de forma íntegra por el sistema.

9 El sistema posee una fuente confiable de tiempo externa que garantiza la integridad del tiempo, de modo que cada apuesta, así como cada evento del sistema se registra con la referencia correcta de tiempo en el que sucede.

10 Es responsabilidad del sistema garantizar la seguridad en las comunicaciones entre las entidades externas como clientes, medios de pago, entidades con derecho legal de acceso a la información de las apuestas de los clientes y distribuidores de información sobre los mercados.

11 Las capacidades de seguridad del sistema se centran en la protección de los datos de carácter personal de los clientes y de las garantías de las apuestas. Para ello, se definen **controles** o **medidas técnicas de seguridad**, entre otras:

- Registro de clientes mediante DNI o formulario;
- Política de I&A y control de acceso de clientes;
- Establecimiento de canales seguros en las comunicaciones;
- Uso de mecanismos criptográficos para garantizar la confidencialidad, integridad y no repudio de las apuestas;
- Uso de mecanismos criptográficos para garantizar la confidencialidad de los datos de los clientes;
- y controles o medidas operacionales, entre otras:
- gestión integral de la seguridad a nivel de sistema con políticas de contratación de operadores internos, copias de respaldo y recuperación del sistema, configuraciones seguras de los componentes de base o que dan soporte a la operación de la aplicación de formalización de las apuestas, cortafuegos e IDS, etc.;
- cumplimiento de la legalidad en el tratamiento de ficheros con información de carácter personal;
- plan de continuidad del negocio;
- medidas de seguridad física de los locales en los que se ubica el STOE.

Uso del STOE

12 El uso del sistema se basa en la funcionalidad asociada a cada tipo de usuario. Se proporcionan diferentes tipos de acceso al sistema:

- Acceso de Clientes: Los clientes son los usuarios que realizan apuestas y deben estar registrados en el sistema. Los clientes tienen acceso a los mercados donde se publican eventos, junto con sus tasas, de modo que pueden apostar, siempre y cuando tengan un saldo en cuenta mayor al

importe de la apuesta a realizar. El cliente firma cada apuesta que hace, de modo que garantiza su autenticidad. Adicionalmente, cada cliente tiene acceso a su saldo, y puede tanto realizar recargas a través de medios de pago, como solicitar reintegros a una cuneta bancaria del total o parte del saldo disponible. Cada cliente puede ver la totalidad de las apuestas que ha realizado.

- Acceso de máquinas de apuestas. En caso de aplicar una arquitectura del sistema de juego basada en la existencia de máquinas de apuestas en las que el cliente final realice la apuesta, existirán medidas de seguridad adicionales respecto al canal de comunicaciones y al mecanismo de firma de las apuestas y boletos. En ambos casos, para garantizar la identidad de la máquina de apuestas se hará uso de un certificado reconocido expedido por el proveedor de servicios de certificación correspondiente.

- Acceso de Operarios internos: Existen usuarios operadores que tienen acceso a la gestión funcional de las apuestas (visualización de apuestas, gestión de riesgos) que se han realizado en el sistema, y a funcionalidad de seguridad asociada a la verificación de la integridad de las apuestas.

- Administradores internos: Los usuarios administradores pueden acceder a los datos de los usuarios del sistema, y pueden crear nuevos usuarios (excepto clientes).

13 Cualquier acceso al sistema es debidamente registrado, y se realiza un control de acceso para cualquier tipo de usuario.

Tipo de STOE

14 El STOE es un sistema operacional cuyo propósito es implantar las capacidades de seguridad necesarias para realizar la gestión integral y formalización de apuestas online, protegiendo los datos de los clientes y las garantías de las apuestas.

Interfaces con otros sistemas requeridos por el STOE

15 La figura representa el diagrama de contexto del sistema, proporcionando los límites en base a las entidades con las que interactúa:

16 El sistema, en su operativa normal, tiene interfaces con las siguientes entidades:

- Clientes o usuarios del sistema.
- Máquinas de apuestas.
- Consejería concreta de la comunidad autónoma correspondiente, que tiene acceso legal a los datos de clientes y apuestas.
- Mercados de eventos, que proporcionan información sobre los eventos activos.
- Medios de pago, a través de los cuales, los clientes pueden recargar el saldo de sus cuentas.

17 La totalidad de los accesos externos se realiza a través de canal seguro.

Organización de dominios

18 La arquitectura de los sistemas operacionales, desde un punto de vista lógico, se estructura en dominios de seguridad o partes (subsistemas y componentes) que están bajo el mismo conjunto de políticas de seguridad.

19 Los requisitos funcionales (técnicos y operacionales) y de garantía se identifican por dominios de seguridad. Cada uno de los dominios que se especifican a continuación implementa sus propias medidas de seguridad bajo una política y contiene su propia política de retribuye a la resolución de una problema de seguridad que se presenta como global en este SPP.

20 Cada dominio tiene sus requisitos de garantía basados en el grado de confianza necesario para ese dominio y su contribución al sistema global. En este SPP, se requiere el mismo grado de confianza en cada uno de los dominios en los que se estructura el sistema, por lo que el conjunto de requisitos de garantía es común para todos ellos.

21 Los dominios presentan interdependencias entre si: existen servicios de seguridad asociados a un dominio, necesarios para ejercitar las capacidades de seguridad de otros. La seguridad se analiza por dominios de seguridad.

22 La arquitectura técnica del sistema que da soporte a los interfaces con las distintas entidades externas, así como la funcionalidad interna de gestión de la seguridad de las apuestas y componentes base, determinan la existencia de aspectos operativos del sistema que se encuentran bajo el paraguas de distintas políticas de seguridad, en concreto, relativas a su funcionalidad y política de control de acceso. Este hecho hace que se establezca una estructura de tres dominios, sin que se puedan considerar estancos:

23 Dos de los dominios, como se puede observar en la figura, operan en el ámbito de la aplicación que proporciona la funcionalidad de formalización de las apuestas: CLIENTES y OPERADORES INTERNOS. El tercer dominio opera en el contexto del soporte lógico, físico y procedimental, que conforma la plataforma base en la operativa del sistema global.

24 Cada dominio incluye sus propios requisitos funcionales técnicos y de control operacional, existiendo para todos ellos un conjunto común de requisitos de control operacional que se detallan en la sección de requisitos de seguridad.

Dominio CLIENTES (y máquinas de apuestas)

25 El dominio **CLIENTES** opera en el contexto de la aplicación de formalización de las apuestas. Se rige por la política de control de acceso asociada a los clientes y presenta capacidades técnicas de seguridad relacionadas con el registro de los clientes, mecanismo técnicos de I&A y control de acceso, funcionalidad que permite a los clientes la gestión de sus datos y sus apuestas, comunicaciones con las pasarelas de pago, un otras entidades externas, etc.

26 Las medidas de seguridad que garantizan la integridad y no repudio de las apuestas realizadas, se basan en la verificación del hash y la firma electrónica de la apuesta. Esta funcionalidad se realiza en el contexto del dominio de OPERADORES INTERNOS. La creación de la firma de la apuesta no se incluye en el dominio de la aplicación, sino que este SPP deja a elección del autor de la SST y desarrollador del STOE, la posibilidad de implementar dentro del mismo la funcionalidad de firma de las apuestas, o que sea el propio cliente del sistema el que proporcione la clave pública y la apuesta firmada al sistema para su verificación.

27 Se encuentran encuadradas en este dominio, las máquinas de apuestas desde las que un cliente final puede realizar la apuesta (a diferencia del cliente que accede desde su ordenador formalpara formalizarla). Aplican los mismos requisitos explicados en el párrafo anterior, con la salvedad de que tanto para el establecimiento del canal seguro (verificación de identidad de la máquina), como para la firma de apuestas y boletos, es obligado el uso de un certificado reconocido, conforme a la Ley 59/2003, de Firma Electrónica, y cuya expedición corresponderá al órgano competente, que podrá externalizar este servicio en un Prestador de Servicios de Certificación.

Dominio OPERADORES INTERNOS

28 El dominio **OPERADORES INTERNOS** opera en el contexto de la aplicación de formalización de las apuestas. Se rige por la política de control de acceso asociada a los operadores internos (operarios de gestión del sistema de apuestas y administradores de seguridad de la aplicación) y presenta capacidades técnicas de seguridad relacionadas con el la administración de clientes, gestión de riesgos, validación de apuestas, comunicaciones seguras con los clientes, garantía de integridad de las apuestas validadas y almacenadas por el sistema, administración de seguridad de la aplicación y auditoría.

Dominio SOPORTE

29 El dominio SOPORTE opera en el contexto del soporte lógico, físico y procedimental, que conforma la plataforma base en la operativa del sistema global. Se rige por su política de control de acceso que incluye, para su implementación, medidas tanto lógicas, como físicas o procedimentales, ya

que, los usuarios en este contexto será todo el personal laboral de la entidad. Presenta capacidades técnicas y de control operacional de seguridad relacionadas con la administración de la seguridad en la plataforma de base de la operativa de la aplicación (instalación segura y mantenimiento de sistemas operativos, bases de datos, cortafuegos, IDS, anti-virus), copias de respaldo y recuperación del sistema, protección de la información almacenada en los sistemas de ficheros y soportes externos, medidas procedimentales relativas al personal, etc.

Declaración de conformidad con respecto a la norma [ISO19791] y [CC31p2]

30 Este SPP declara conformidad con:

- La norma ISO/IEC TR 19791 Information technology – Security techniques – Security assessment of operational systems. Se declara conformidad funcional y de garantía (no extendidas).
- Common Criteria for Information Technology Security Evaluation, versión 3.1 R3 Jul 2009.

Conformidad de otros PP

31 No se declara conformidad con ningún SPP.

Definición del problema de seguridad

32 La definición del problema de seguridad detallada en esta sección, es común para los tres dominios declarados en la sección Organización de dominios.

Activos del STOE

33 El sistema operacional deberá proteger los datos de carácter personal de los clientes y las garantías de sus las apuestas. Los activos que protege el sistema son:

ACTIVOS	DESCRIPCIÓN
DATOS-CLIENTES	Datos de los clientes registrados en el sistema, entre otros: ○ Nombre. ○ Apellidos. ○ Fecha de nacimiento. ○ DNI/NIF ○ Dirección postal. ○ Código Postal. ○ País. ○ Email. ○ Teléfono móvil. ○ Nombre de usuario. ○ Pregunta de seguridad. ○ Número de Cuenta Bancaria. Datos de clientes potenciales para llevar a cabo nuevas acciones comerciales y prospección comercial. Datos pertenecientes a los clientes obtenidos a través de la relación comercial y que están almacenados el sistema.
DATOS-APUESTAS	Datos de las apuestas realizadas por los clientes, entre otros: ○ Identificación de la apuesta.

	○ Usuario que realiza la apuesta. ○ Nombre del resultado de la apuesta. ○ Nombre del mercado de la apuesta (+ identidad de la entidad tercera parte). ○ Cuota de la apuesta en el portal. ○ Cuota de la apuesta en la entidad tercera parte. ○ Cantidad de la apuesta en el portal. ○ Cantidad de la apuesta en en la entidad tercera parte. ○ Ganancia obtenida por la apuesta. ○ Fecha de realización de la apuesta. ○ Fecha de realización del evento. ○ Estado de la apuesta. ○ Identificador Resultado del Gestor de Riesgos. ○ Identificador del Libro del Gestor de Riesgos. ○ Identificador del Mercado del Gestor de Riesgos. ○ Apuesta premiada o no. ○ Identificador de resultado devuelto por en la entidad tercera parte. ○ Parámetro de resultado de en la entidad tercera parte. ○ Identificador del deporte de la apuesta. ○ Descripción del deporte de la apuesta. ○ Identificador del mercado de la apuesta. ○ Fecha de cancelación de la apuesta. ○ Ruta de mercado de la apuesta. ○ Nombre del resultado de la apuesta. Estos datos permiten que el sistema operacional realice la gestión de las apuestas realizadas por los clientes en la plataforma de juego, resolución y resultados, transacciones, formas de pago, etc.
DATOS-BOLETOS	Datos del boleto asociado a la apuesta formalizada y que se envía al cliente, entre otros:

	○ Identificación de la empresa autorizada. ○ Acontecimiento sobre el que se apuesta y fecha del mismo. ○ Modalidad e importe de la apuesta realizada. ○ Coeficiente de la apuesta, en su caso. ○ Pronóstico realizado. ○ Hora, día, mes y año de formalización de la apuesta. ○ Número o combinación alfanumérica que permita identificarlo con carácter exclusivo y único. ○ Identificación del medio de formalización de las apuestas utilizado.
SERVICIO	Se corresponde con el servicio que el sistema operacional proporciona a los clientes para la gestión de sus datos personales y de sus apuestas. Los DATOS-CLIENTES se recogen en el sistema con el fin de gestionar las apuestas que realicen los clientes.

34 Como se deriva de los ejemplos de contenido de los activos DATOS-CLIENTES y DATOS-APUESTAS de la tabla anterior, parte de la información se corresponde con datos de carácter personal que están sujetos a las medidas de seguridad especificadas en [RMS] para un nivel de seguridad BÁSICO según se define en [LOPD].

35 Por lo tanto, se considera dicha información, como activos que debe proteger el sistema. El valor de los activos se centra en la confidencialidad (excepto boletos), integridad y disponibilidad de los mismos.

36 En el caso de las apuestas y boletos, también se considera el "no repudio" como valor que debe garantizarse.

37 Así mismo, el propio SERVICIO de apuestas es un activo para el que debe garantizarse su disponibilidad.

38 La siguiente tabla resume los activos y el valor del mismo que se desea proteger:

Activo	**Valor**
DATOS-CLIENTES	Confidencialidad, Integridad, Disponibilidad
DATOS-APUESTAS	Confidencialidad, Integridad, Disponibilidad,

	No repudio
DATOS-BOLETOS	Integridad, Disponibilidad, No repudio
SERVICIO	Disponibilidad

Definición del riesgo

39 En esta sección se define el riesgo (aceptable / no-aceptable) en términos de las amenazas sobre los activos, definiendo el agente de la amenaza (experiencia, recursos, oportunidad y motivación), activos afectados y acción adversa o vulnerabilidad. Las amenazas tienen como objeto eliminar el valor del activo, por lo que se supone:

Activo	Estado del riesgo	Valor Comprometido
DATOS-CLIENTES	riesgo no-aceptable	Confidencialidad
	riesgo no-aceptable	Integridad
	riesgo no-aceptable	Disponibilidad
DATOS-APUESTAS	riesgo no-aceptable	Confidencialidad
	riesgo no-aceptable	Integridad
	riesgo no-aceptable	Disponibilidad
	riesgo no-aceptable	No repudio
DATOS-BOLETOS	riesgo no-aceptable	Integridad
	riesgo no-aceptable	No repudio
	riesgo no-aceptable	Disponibilidad
SERVICIO	riesgo no-aceptable	Disponibilidad

40 En la tabla anterior, para el riesgo asociado a la **disponibilidad** de los DATOS-CLIENTES, DATOS-APUESTAS, DATOS-BOLETOS y SERVICIO, se dan ciertos escenarios de ataque, por ejemplo, el robo de los servidores que almacenan los datos y proporcionan el servicio o un incendio en las

instalaciones, en los que la materialización u ocurrencia del ataque y eliminación del valor del activo, se contrarresta con una combinación de medidas técnicas y operacionales implementadas a posteriori del incidente de seguridad. Es decir, se implementan medidas correctivas que, combinadas con medidas preventivas, disminuyen el efecto final (no evitan el suceso) y que tienen como objetivo, la recuperación del sistema en un tiempo breve y sin pérdida de datos.

41 En todos los escenarios, se supone un **riesgo no-aceptable**, en la medida en que se espera que sistema implemente controles técnicos y operacionales de carácter preventivo (y correctivo) que eliminen las amenazas definidas.

42 Los agentes de la amenaza, en función del origen del ataque podrán ser:

- (AG1) Agentes que realizan ataques remotos a través del cable y que podrán ser tanto clientes registrados, como usuarios no registrados. En dichos ataques, el punto de entrada es siempre el interface exterior. Estos atacantes pueden tener alta motivación ya que la posible manipulación de apuestas podría proporcionar grandes beneficios monetarios, por lo que aumenta la probabilidad de existencia del ataque. Esta alta motivación podría suponer el acceso a recursos tanto técnicos como personales de alta cualificación. La oportunidad se podría clasificar como de acceso ilimitado, ya que el acceso remoto al sistema se realiza a través de redes públicas.

- (AG2) Agentes que realizan ataques que implican un acceso físico a los locales donde se ubica el sistema operacional con el objeto de robar o destruir la información. Estos atacantes pueden tener alta motivación ya que la posible manipulación de apuestas o reclamaciones fraudulentas podrían proporcionar grandes beneficios monetarios, por lo que aumenta la probabilidad de existencia del ataque. Esta alta motivación podría suponer el acceso a recursos tanto técnicos como personales de alta cualificación. La oportunidad se podría clasificar como de acceso moderado ya que existe un acceso único para realizar el acto de robo o de sabotaje.

- (AG3) Agentes naturales cuyo efecto sería la destrucción de la información (por ejemplo, incendios no provocados, inundaciones no provocadas, terremotos, etc…). No es aplicable la determinación de motivación, recursos, experiencia u oportunidad al ser en evento natural. Sí se considera de interés que el autor de la SST y desarrollador del sistema, realicen un estudio de la probabilidad de existencia de eventos naturales en función de la localización del local.

43 A continuación se detallan las amenazas definiendo la acción adversa, los activos comprometidos, su valor y el agente que la realiza.

Amenaza	Acción adversa	Activo/valor comprometido	Agente
T-REMOTO	Un atacante (usuario registrado o no) accede de manera remota a los datos de las apuestas de los clientes con el objeto de vulnerar su integridad o eliminar la prueba de no repudio en origen. En el caso de usuario registrado puede intentar manipular sus propias apuestas o intentar acceder a los datos de otro cliente o apuestas para comprometer su confidencialidad o integridad.	Confidencialidad, integridad y disponibilidad de DATOS-CLIENTES. Confidencialidad, integridad, disponibilidad y no repudio de DATOS-APUESTAS Integridad, disponibilidad y no repudio de DATOS-BOLETOS Disponibilidad de SERVICIO	AG 1
T-LOCAL	Un atacante accede de manera local/física y roba o sabotea los servidores que alojan el sistema lógico y físico (copias de respaldo ubicadas en el propio local) y la información a proteger.	Confidencialidad y disponibilidad de DATOS-CLIENTES. Confidencialidad, disponibilidad y no repudio de DATOS-APUESTAS Integridad, disponibilidad y no repudio de DATOS-BOLETOS Disponibilidad de SERVICIO	AG 2
T-NATURAL	Un agente natural causa la destrucción de los servidores que alojan el sistema lógico y físico (copias de respaldo ubicadas en el propio local) y la información a proteger.	Disponibilidad de DATOS-CLIENTES. Disponibilidad DATOS-APUESTAS Disponibilidad y no repudio de DATOS-BOLETOS Disponibilidad de SERVICIO	AG 3

44 El compromiso de la confidencialidad, integridad, disponibilidad y no repudio de los activos en las amenazas T-REMOTO, T-LOCAL y T-NATURAL, se considera **riesgo no-aceptable** en todos los casos y con las consideraciones hechas anteriormente.

Políticas organizativas

45 Las políticas organizativas son un conjunto de reglas, procedimientos o guías de operación impuestas por la organización para la operación real del sistema.

46 A continuación se especifican las políticas organizativas que deberán ser tenidas en cuenta.

Política	Descripción
OSP-REGISTRO	El registro de un cliente se deberá poder realizar mediante: ○ DNIe. Este modo de auto-registro utilizará el dni electrónico como fuente de validación de la identidad del usuario. ○ Formulario. Este modo de auto-registro utilizará un formulario web de registro como fuente de obtención de la identidad del usuario.
OSP-I&A	Se proporcionarán los siguientes mecanismos de I&A: ○ DNIe. Este método de autenticación utilizará el dni electrónico como fuente de validación de la identidad del usuario. ○ Usuario/contraseña. Este método de autenticación utilizará el usuario y la contraseña como fuente de validación de la identidad del usuario.
OSP-LOPD	Los datos de carácter personal contenidos en los "ficheros" de clientes y apuestas (y otros si aplicara), deberán ser tratados conforme a las disposiciones de [LOPD] y con las medidas de seguridad especificadas en [RMS] para el nivel de seguridad BÁSICO.
OSP-NOEVIL	Se dispondrán cuantas medidas de control operacionales se consideren necesarias para garantizar que los operadores internos del sistema

	sean confiables y no incurran intencionadamente o no, en situaciones que comprometan la seguridad de los activos (garantías en la contratación del personal, establecimiento de compromisos de confidencialidad, formación en seguridad, revisión de la auditoría, etc.).
OSP-BCP	La entidad establecerá un plan de continuidad del servicio en que se definan las situaciones de crisis y medidas de recuperación del sistema que garanticen la continuidad de la actividad. Ante la ocurrencia de cualquier evento que ponga en peligro la continuidad del servicio, se garantizará que el personal necesario para garantizar la continuidad estará presente en las instalaciones no más tarde de los 25 minutos posteriores a la ocurrencia del evento. La recuperación del sistema deberá garantizar la inexistencia de pérdida de transacciones realizadas y una disponibilidad del servicio del 99'96 % (máximo 15 min. al mes de caida).
OSP-RND	Aleatoriedad en las apuestas. Se deberá ganartizar criterios de aleatoriedad para aquellas apuestas en las que así se precise. La generación de los datos se realizará de forma aleatoria e imprevisible ([RACC]).
OSP-STAMP	Las apuestas tendrán asociadas una medida de tiempo fiable.
OSP-TRAZA	Se proporcionarán mecanismos que permitan seguir o rastrear el registro de las operaciones de apuestas realizadas.

Objetivos de seguridad

47 La especificación de los objetivos de seguridad que se detallan en esta sección y que resuelven el problema de seguridad definido en la sección Definción del Problema de Seguridad, es común para los tres dominios declarados en la sección Organización de dominios.

Objetivos de seguridad funcionales del STOE

Objetivos Funcionales STOE	Descripción
OF-INT	Garantizar la integridad de los datos de los clientes, apuestas y boletos.
OF-CONF	Garantizar la confidencialidad de los datos de los clientes y de las apuestas.
OF-DISP-DATOS	Garantizar la disponibilidad de los datos de los clientes, apuestas y boletos.
OF-NOREP-DATOS	Garantizar el no repudio en origen de las apuestas realizadas por los clientes y el no repudio en origen de los boletos enviados por la entidad a los clientes. De esta forma se garantiza el no repudio en origen y destino de las apuestas realizadas.
OF-DISP-SERV	Garantizar una disponibilidad del servicio del 99'96 % (máximo 15 min. al mes de caida).
OF-REGISTRO	Proporcionar un sistema de registro de los clientes mediante: o DNIe. Este modo de auto-registro utilizará el dni electrónico como fuente de validación de la identidad del usuario. o Formulario. Este modo de auto-registro utilizará un formulario web de registro como fuente de obtención de la identidad del usuario.

OF-I&A	Proporcionar los siguientes mecanismos de I&A: o DNIe. Este método de autenticación utilizará el dni electrónico como fuente de validación de la identidad del usuario. o Usuario/contraseña. Este método de autenticación utilizará el usuario y la contraseña como fuente de validación de la identidad del usuario.
OF-LOPD	Tratar los datos de carácter personal contenidos en los "ficheros" de clientes y apuestas (y otros si aplicara), conforme a las disposiciones de [LOPD] y con las medidas de seguridad especificadas en [RMS] para el nivel de seguridad BÁSICO.
OF-NOEVIL	Disponer medidas de de control operacionales necesarias para garantizar que los operadores internos del sistema sean confiables y no incurran intencionadamente o no, en situaciones que comprometan la seguridad de los activos (garantías en la contratación del personal, establecimiento de compromisos de confidencialidad, formación en seguridad, revisión de la auditoría, etc.).
OF-BCP	Establecer un plan de continuidad del negocio en que se definan las situaciones de crisis y medidas de recuperación del sistema que garanticen la continuidad de la actividad. El plan deberá tener en cuenta los siguientes aspectos: • Ante la ocurrencia de cualquier evento que ponga en peligro la continuidad del servicio, se garantizará que el personal técnico estará presente en las instalaciones no más tarde de los 25 minutos posteriores a la ocurrencia del evento. • La recuperación del sistema deberá garantizarla inexistencia de pérdida de transacciones.
OF-RND	Garantizar criterios de aleatoriedad para aquellas apuestas en que así se precise.
OF-STAMP	Asociar una medida de tiempo fiable a las apuestas formalizadas.

OF-TRAZA	Establecer un sistema de registrode eventos que rastrear las operaciones de apuestas realizadas y garantizar la integridad de los registros obtenidos.

Objetivos de seguridad funcionales de sistemas operacionales externos

Objetivos Funcionales Entidades	Descripción
OE-COM	Las entidades externas establecerán o aceptarán el establecimiento de un canal seguro en las comunicaciones con el STOE para garantizar la autenticidad de ambas partes, y confidencialidad de las comunicaciones. Ejemplos de entidades externas que deben considerarase: ○ Clientes o máquinas de apuestas ○ Consejería de la Comunidad ○ Pasarelas de Pago
OE-FIRMA	OPCIONAL (imputable al STOE) En el caso del cliente será responsable de realizar el hash y firma electrónica de las apuestas conforme a los requisitos criptográficos de STOE, para garantizar la integridad y no repudio de las apuestas que realice.

Objetivos de seguridad de garantía del STOE

48 Se establecen objetivos de seguridad para la declaración de seguridad del sistema (SST) y para el propio STOE cubriendo todas las fases del ciclo de vida del sistema:

- Desarrollo / Integración
- Instalación
- Operación

- Modificación

Objetivos Garantía STOE	Descripción
OA-ASS	Evaluar la SST.
OA-AOD	Evaluar las guías de operación del sistema.
OA-ASD	Evaluar el diseño de arquitectura del sistema operacional y la documentación de configuración.
OA-AOC	Validar la gestión de configuración del sistema operacional.
OA-AOT	Realizar pruebas del sistema operacional.
OA-AOV	Realizar el análisis de vulnerabilidades del sistema operacional en el que el potencial de ataque del atacante sea "**Moderate**" conforme al nivel de motivavión y demás características especificadas para los distintos perfiles de agentes de la amenaza definidos en la sección Definición del problema de seguridad.
OA-APR	Evaluar las actividades de gestión desarrolladas para la preparación para la operación real del sistema.
OA-ASO	Evaluar el sistema de registro y monitorización.

Justificación de los objetivos de seguridad

49 Las tablas que se exponen a continuación detallan el mapeo amenazas y OSPs vs. objetivos funcionales del STOE y objetivos funcionales de sistemas externos.

Amenaza	Objetivos Funcionales STOE	Objetivos Funcionales de Sistemas Externos
T-REMOTO	OF-INT OF-CONF	OE_COM OE_FIRMA (si no lo

	OF-DISP-DATOS OF-NOREP-DATOS OF-DISP-SERV	implementa STOE)
T-LOCAL	OF-CONF OF-DISP-DATOS OF-NOREP-DATOS OF-DISP-SERV	OE_FIRMA (si no lo implementa STOE)
T-NATURAL	OF-DISP-DATOS OF-NOREP-DATOS OF-DISP-SERV	OE_FIRMA (si no lo implementa STOE)

Política	**Objetivos Funcionales STOE**
OSP-REGISTRO	OF-REGISTRO
OSP-I&A	OF-I&A
OSP-LOPD	OF-LOPD
OSP-NOEVIL	OF-NOEVIL
OSP-BCP	OF-BCP OF-DISP-SERV
OSP-RND	OF-RND
OSP-STAMP	OF-STAMP
OSP-TRAZA	OF-TRAZA

50 Los objetivos de garantía seleccionados proporcionarán la garantía adecuada en la evaluación de las capacidades del sistema. Se ha elegido un nivel de potencial de ataque "**Moderate**", por el nivel de motivación del atacante definido.

Definición de componentes extendidos

51 Se define el componente extendido FCS_RNG para especificar el requisito que satisfaga los criterios de aleatoriedad para aquellas apuestas en las que así se precise. La generación de los datos se realizará de forma aleatoria e imprevisible, tal y como se requiere en [RACC].

52 La especificación del componente requiere la definición de una nueva familia dentro de la clase FCS de soporte a las funciones criptográficas.

Definición de la familia FCS_RNG.

53 Comportamiento de la familia

Ésta familia define requisitos para la generación de números aleatorios siempre que éstos se utilicen para una finalidad criptográfica.

54 Relaciones de jerarquía entre los componentes de la familia

La familia presenta un único componente.

FCS_RNG.1 La generación de números aleatorios requiere que los números aleatorios cumplan una métrica de calidad definida.

55 Gestión: FCS_RNG.1

No se definen actividades de gestión.

56 Auditoría: FCS_RNG.1

No se definen acciones auditables.

57 **FCS_RNG.1 Generación de números aleatorios**

Jerárquico a: No hay otros componentes.

Dependencias: FPT_TST.1.

FCS_RNG.1.1 La TSF deberá proporcionar un [selección: determinístico, no-determinístico] generador de números aleatorios que cumpla [asignación: lista de las características de seguridad].

FCS_RNG.1.2 La TSF deberá proporcionar números aleatorios que cumplan [asignación: una métrica de calidad definida].

Requisitos de seguridad del STOE

58 En todos los requisitos técnicos derivados de [CC31p2] que se incluyen en esta sección, se han realizado de manera genérica los siguientes refinamientos:

- existen requisitos en los que el control implica tanto requisitos de carácter técnico como requisitos de carácter operacional. En estos casos, se ha sustituido el acrónimo TSF (TOE Security Functionality), por el acrónimo SSF (System Security Functionality) indicando la posible combinación entre TSF y OSF;
- sustitución del término TOE (Target Of Evaluation), por STOE (System Target of Evaluation);
- traducción de los requisitos al español, manteniendo el espíritu de los mismos tal y como se redactan en [CC31p2].

Requisitos que aplican a los tres dominios

REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL

Auditoría

FOS_MON.1 Registros de auditoría

59 Dependencias: no existen dependencias.

60 FOS_MON.1.1 La OSF deberá planificar [asignación: requisitos de seguridad] para la auditoria y aquellas actividades que impliquen comprobaciones en los sistemas operacionales y estará de acuerdo con minimizar el riesgo de interrupción de los procesos de negocio.

61 FOS_MON.1.2 La OSF deberá definir [asignación: requisitos de seguridad] en la auditoria con la gestión apropiada.

62 FOS_MON.1.3 La SSF deberá producir [asignación: monitorización] de las actividades del administrador del sistema y del operador del sistema. Los registros incluirán la hora en la que el evento o fallo ocurrió, la información acerca del evento o fallo, qué cuenta y qué administrador u operador estuvieron involucrados, además de todos los cambios en el equipo, software y procedimientos.

63 FOS_MON.1.4 La OSF deberá definir [asignación: reglas] para registrar el equipo que salga de una sesión y que vuelva a reiniciar la sesión.

64 FOS_MON.1.5 La OSF deberá definir [asignación: requisitos de seguridad] para la monitorización de la copia y el uso de la información operacional para proporcionar un registro de auditoría.

65 FOS_MON.1.6 La OSF deberá definir [asignación: procedimientos] de recogida de registros de auditoria y evidencias similares.

66 FOS_MON.1.7 La OSF deberá definir [asignación: requisitos de seguridad] para el mantenimiento de un registro de todas las extracciones de los dispositivos removibles de la organización para mantener un registro de auditoría.

67 FOS_MON.1.8 La OSF establecerá [asignación: procedimientos] de monitorización del uso de las instalaciones de proceso de información, además de revisar los resultados de las actividades de monitorización regularmente.

68 FOS_MON.1.9 La SSF deberá proporcionar [asignación: medidas de seguridad] para proteger las instalaciones donde se produce la monitorización y los registros de información para evitar su alteración y el acceso no autorizado.

69 FOS_MON.1.10 La SSF deberá producir [asignación: procedimientos] de monitorización y análisis de fallos, y llevar a cabo las acciones correspondientes.

70 **Nota de aplicación:**

- En el dominio SOPORTE se generarán los eventos de auditoría tal y como se definen en el requisito FAU_GEN.1 / SOPORTE. La medida de tiempo que se asigna se obtendrá de una fuente fiable, tal y como se especifica en FPT_STM.1 / SOPORTE. Esta auditoria forma parte del IDS que debe implementar el STOE. Se obliga por política (OSP) a la revisión de los logs regularmente.

- En los dominios CLIENTES y OPERADORES INTERNOS se definen también eventos de auditoría (FAU_GEN.1 / CLIENTES y FAU_GEN.1 / OPERADORES respectivamente) que también estarán sujetos a revisión (en este caso, por parte de los administradores del dominio OPERADORES INTERNOS).

- Las medidas de protección de la información de auditoría implican una combinación de medidas técnicas y de control operacional: mecanismos de I&A, políticas de control de acceso y medidas de seguridad físicas en los dominios OPERADORES INTERNOS y SOPORTE (FOS_MON.1.9).

- FOS_MON.1.10: se especificarán procedimientos para el análisis de los logs generados en el dominio de OPERADORES INTERNOS y SOPORTE, y acciones en caso de fallo.

Protección de datos

FOA_PRO.1 Privacidad de los datos

71 Dependencias: no existen dependencias.

72 FOA_PRO.1.1 La OSF deberá definir [asignación: reglas] para no usar las bases de datos operacionales que contengan datos de carácter personal cuando la finalidad sea su prueba.

73 FOA_PRO.1.2 La OSF deberá definir [asignación: reglas] para obtener información de dominio público de acuerdo con la legislación de protección de datos de carácter personal, para procesarla completamente y de forma precisa, y para protegerla durante el proceso de obtención y almacenamiento.

74 FOA_PRO.1.3 La OSF deberá definir [asignación: responsabilidades y reglas] del propietario de los datos para informar al oficial autorizado de la organización responsable de los datos de carácter personal sobre el propósito del almacenamiento de los datos de carácter personal, y para asegurar que tiene el conocimiento relativo a la protección de datos de carácter personal definida en la legislación correspondiente.

75 **Nota de aplicación:**

- La obtención de datos de carácter personal en la operación del sistema de formalización de apuestas estará sujeta a los requisitos de la [LOPD] y medidas de protección de los datos especificadas en [RMS], para un nivel de seguridad de los datos BÁSICO.

- Se deberán garantizar los derechos de los interesados en el ámbito de la calidad de los datos recogidos, el derecho de información en la recogida de los datos, el consentimiento del afectado, datos especialmente protegidos, el deber de secreto, comunicación y acceso a los datos por cuenta de terceros y derechos de acceso, rectificación, cancelación y oposición. Todo ello teniendo en cuenta la clasificación del nivel de seguridad de los datos BÁSICO, definida conforme a la tipología especificada en [LOPD].

FOA_INF.1 Protección de datos

76 Dependencias: FOS_POL.1 Requisitos de seguridad

77 FOA_INF.1.1 La OSF deberá definir [asignación: directrices] en la retención, almacenamiento, manejo y destrucción de registros e información.

78 FOA_INF.1.2 La OSF deberá definir [asignación: reglas] para la planificación del tiempo en que son retenidos, identificando los tipos de registros esenciales y el periodo de tiempo para el cual deberían ser retenidos.

79 FOA_INF.1.3 La OSF deberá definir [asignación: procedimientos] para permitir la destrucción apropiada de los registros después de un periodo determinado si no son de utilidad para la organización.

80 FOA_INF.1.4 La SSF deberá proporcionar [asignación: medidas] para que la información sea destruida, borrada y sobrescrita utilizando técnicas aprobadas para dispositivos que contienen información sensible.

81 FOA_INF.1.5 La SSF deberá proporcionar [asignación: medidas] para las comunicaciones electrónicas protegiendo los mensajes de accesos no autorizados, modificación o denegación de servicios, asegurando un correcto tratamiento y transporte del mensaje, fiabilidad y disponibilidad del servicio, y sujeto a las consideraciones legales.

82 FOA_INF.1.6 La OSF deberá definir [asignación: procedimientos] para el etiquetado y manejo de la información incluyendo tanto el formato físico como electrónico de acuerdo con el esquema de clasificación adoptado por la organización.

83 FOA_INF.1.7 La OSF deberá definir [asignación: reglas] para la identificación de privilegios asociados con cada producto del sistema y cada aplicación, y las categorías de personal a los que necesitan ser asignados.

84 FOA_INF.1.8 La OSF deberá definir [asignación: reglas] para la asignación de privilegios a usuarios en base a la necesidad de uso y en base a evento por evento de acuerdo a la política de control de acceso.

85 FOA_INF.1.9 La OSF deberá definir [asignación: requisitos de seguridad] para proteger la información usada en comercio electrónico y que se transmite por redes pública, de: actividades fraudulentas, contenciosos en contratos y revelación y modificación no autorizada.

86 **Nota de aplicación:**

- La obtención de datos de carácter personal en la operación del sistema de formalización de apuestas estará sujeta a los requisitos de la [LOPD] y medidas de protección de los datos especificadas en [RMS] con un nivel de seguridad BÁSICO.

- Los datos de carácter personal que se encuentren en los ficheros responderán a la finalidad para la que fueron obtenidos, no siendo posible un uso no previsto de los mismos, deberán ser exactos y deberán estar puestos al día. Deberán ser obtenidos de forma lícita.

- Los datos de carácter personal no deberán mantenerse indefinidamente sin justificación. Se deberán establecer procedimientos para la eliminación de los datos en el momento en que la ley no exija su mantenimiento en el sistema (FOA_INF.1.1,..., FOA_INF.1.4). Estos procedimientos tendrán en cuenta la existencia de datos tanto en la base de datos del sistema, como en las copias de respaldo.

- Las políticas de control de acceso definidas para los tres dominios de seguridad (CLIENTES, OPERADORES INTERNOS y SOPORTE) especifican las reglas que deberán garantizar la protección de los datos.

- Se deberán definir los requisitos de seguridad en la realización de operaciones de comercio electrónico, teniendo en cuenta los mecanismos de seguridad que implementan las distintas pasarelas de pago existentes. Los requisitos se identifican en **FTP_ITC.1 Canal seguro Inter-TSF / PASARELA DE PAGO.**

Dominio CLIENTES

REQUISITOS FUNCIONALES TÉCNICOS

Requisitos de Identificación y autenticación.

FIA_UID.2 Identificación de usuario antes de cualquier acción / CLIENTES

87 Jerárquico a: FIA_UID.1 Momento de la identificación

88 Dependencias: no existen dependencias.

89 FIA_UID.2.1 La TSF deberá requerir que cada usuario se identifique con éxito antes de permitirle cualquier acción en la que intervenga la TSF en nombre de ese usuario.

FIA_UAU.2 Autenticación de usuario antes de cualquier acción / CLIENTES

90 Jerárquico a: FIA_UAU.1 Momento de la autenticación

91 Dependencias: FIA_UID.1 Momento de la identificación

92 FIA_UAU.2.1 La TSF deberá requerir que cada usuario se autentique con éxito antes de permitirle cualquier acción en la que intervenga la TSF en nombre de ese usuario.

FIA_UAU.5 Mecanismos de autenticación múltiples / CLIENTES

93 Jerárquico a: No hay otros componentes.

94 Dependencias: no existen dependencias.

95 FIA_UAU.5.1 La TSF deberá proporcionar [asignación: lista de múltiples mecanismos de autenticación] para soportar la autenticación de usuario.

96 FIA_UAU.5.2 La TSF deberá autenticar la identidad reclamada por el usuario de acuerdo a [asignación: reglas que describan cómo los diversos mecanismos de autenticación proporcionan autenticación].

97 **Nota de aplicación:**

- La asignación en el primer elemento deberá especificar al menos los siguientes mecanismos de autenticación:
    - DNIe: Este método de autenticación utilizará el dni electrónico como fuente de validación de la identidad del usuario. Para poder acceder a los

certificados del DNIe, **será necesario que el usuario introduzca el PIN** del mismo, pudiendo obtener de esta manera los datos del DNIe

- Usuario/contraseña: Este método de autenticación utilizará el usuario y la contraseña como fuente de validación de la identidad del usuario.

FIA_AFL.1 Manejo de fallos de autenticación / CLIENTES

98 Jerárquico a: No hay otros componentes.

99 Dependencias: FIA_UAU.1 Momento de la autenticación

100 FIA_AFL.1.1 La TSF deberá detectar cuando se producen [3] intentos de autenticación sin éxito relativos a [clientes intentando autenticarse remotamente con usuario/contraseña].

101 FIA_AFL.1.2 Cuando el número definido de intentos de autenticación sin éxito haya sido [alcanzado], la TSF deberá [bloquear la cuenta del cliente].

Requisitos de protección de datos de usuario

FDP_ACC.2 Control de acceso completo / CLIENTES

102 Jerárquico a: FDP_ACC.1 Subconjunto del control de acceso

103 Dependencias: FDP_ACF.1 Atributo de seguridad basado en el control de acceso

104 FDP_ACC.2.1 La TSF deberá hacer cumplir [política de control de acceso de clientes] en [Sujetos: clientes; Objetos: fichero apuestas, ficheros clientes] y para todas las operaciones entre sujetos y objetos cubiertas por la SFP.

105 FDP_ACC.2.2 La TSF deberá asegurar que todas las operaciones entre sujetos controlados por la TSF y cualquier objeto controlado por la TSF están cubiertos por el control de acceso de la SFP.

FDP_ACF.1 Control de acceso basado en atributos de seguridad / CLIENTES

106 Jerárquico a: No hay otros componentes.

107 Dependencias:

108 FDP_ACC.1 Subconjunto del control de acceso

109 FMT_MSA.3 Inicialización de atributos estática

110 FDP_ACF.1.1 La TSF deberá hacer cumplir la [política de control de acceso de clientes] a objetos basada en: [

- Sujetos: clientes; atributos: identidad del cliente;
- Objetos:
  - fichero apuestas; sin atributos;
  - ficheros clientes; sin atributos;]

111 FDP_ACF.1.2 La TSF deberá hacer cumplir las siguientes reglas para determinar si una operación entre sujetos controlados y objetos controlados es permitida: [se concederá acceso si el cliente tiene los permisos necesarios para acceder a sus apuestas o a sus datos personales].

112 FDP_ACF.1.3 La TSF deberá autorizar explícitamente el acceso de sujetos a objetos basado en las siguientes reglas adicionales: [asignación: reglas, basaas en los atributos de seguridad, que explícitamente autorizan el acceso de sujetos a objetos].

113 FDP_ACF.1.4 La TSF deberá denegar explícitamente el acceso de sujetos a objetos basado en las siguientes reglas adicionales: [asignación: reglas, basadas en los atributos de seguridad, que explícitamente deniegan el acceso de sujetos a objetos].

114 **Nota de aplicación:**

- La política de control de acceso deberá garantizar que un determinado cliente (autenticado) sólo pueda acceder a sus apuestas y datos personales. La identidad del cliente se asigna cuando éste realiza el autoenrollment o registro. La identidad permanece asociada al cliente hasta que la ley permita borrar dicho registro. No se realiza gestión de los atributos de seguridad de la política, por lo que no es necesario, satisfacer las dependencias FMT_MSA.3 y FMT_MSA.1.

- En el caso de existir otra entidad involucrada en esta política de control de acceso, por ejemplo, la consejería, ésta tendrá que ampliarse para recogerla.

Funciones de gestión de la seguridad

FMT_SMF.1 Especificación de las Funciones de Gestión / CLIENTES

115 Jerárquico a: No hay otros componentes.

116 Dependencias: no existen dependencias.

117 FMT_SMF.1.1 La TSF deberá ser capaz de realizar las siguientes funciones de gestión: [

- registro de clientes;
- cambio de contraseña;
- asignación: lista de funciones de gestión que serán proporcionadas por la TSF].

118 **Nota de aplicación:**

- El registro se deberá poder realizar mediante:
  - DNIe:
    - Este modo de auto-registro utilizará el dni electrónico como fuente de validación de la identidad del usuario.
    - Para poder acceder a los certificados del DNIe, será necesario que el usuario introduzca el PIN del mismo, pudiendo obtener de esta manera los datos de Nombre, Apellidos, Fecha de nacimiento y nº de dni.
  - Formulario:
    - Este modo de auto-registro utilizará un formulario web de registro como fuente de obtención de la identidad del usuario.

Comunicaciones

Pasarelas de pago

FTP_ITC.1 Canal seguro Inter-TSF / PASARELA DE PAGO

119 Jerárquico a: No hay otros componentes.

120 Dependencias: no existen dependencias.

121 Refinamiento:

122 FTP_ITC.1.1 La TSF deberá proporcionar un canal de comunicación entre ella y otro producto de las TI seguro que sea lógicamente distinto de otros canales de comunicación y proporcione identificación asegurada en sus puntos finales, además de protección de los datos del canal contra modificación o revelación.

123 FTP_ITC.1.2 La TSF deberá permitir [el sistema de apuestas] iniciar la comunicación a través del canal seguro.

124 FTP_ITC.1.3 La TSF deberá iniciar la comunicación a través del canal seguro para [provisión de fondos para las apuestas, selección: otras operaciones como el reintegro de cantidades].

125 **Nota de aplicación:**

- Se requiere un canal seguro en las comunicaciones con los medios de pago para el pago de las cantidades apostadas por los clientes, o para el reintegro de cantidades ganadas por el cliente. Existen casos en los que este reintegro se realiza mediante un medio de pago con banca electrónica o también podría realizarse con una transferencia directa con el banco asociado al cliente.

Auditoría

FAU_GEN.1 Generación de datos de auditoría / CLIENTES

126 Jerárquico a: No hay otros componentes.

127 Dependencias: FPT_STM.1 Sellados de tiempo fiables

128 FAU_GEN.1.1 La TSF deberá ser capaz de generar un registro de auditoría de los siguientes eventos auditables:

a) Inicio y finalización de las funciones de auditoría;

b) Todos los eventos auditables para el [sin especificar] nivel de auditoría; y

c) [login del cliente, apuestas realizadas, cambio de datos personales, movimientos de cuenta, asignación: otros eventos auditables específicamente definidos].

129 FAU_GEN.1.2 La TSF deberá registrar dentro de cada registro de auditoría al menos la siguiente información:

a) fecha y hora del evento, tipo de evento, identidad del sujeto (si es aplicable), y el resultado (éxito o fallo) del evento; y

b) Para cada tipo de evento, basado en las definiciones de eventos auditables de los componentes funcionales incluidos en el Perfil de Protección/Declaración de seguridad del sistema, [asignación: otra información relevante de auditoría].

FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES

130 Jerárquico a: No hay otros componentes.

131 Dependencias: Generación de datos de auditoría / CLIENTES

132 FAU_STG.1.1 La TSF deberá proteger los registros de auditoria almacenados en la traza de auditoría contra el borrado no autorizado.

133 FAU_STG.1.2 La TSF deberá ser capaz de [selección, elegir uno de: evitar, detectar] unauthorised modifications to the stored audit Registros in the audit trail.

REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL

134 No existen requisitos de control operacional en el dominio CLIENTES adicionales a los especificados en la sección de requisitos operacionales comunes a los tres dominios.

Dominio OPERADORES INTERNOS

REQUISITOS FUNCIONALES TÉCNICOS

Requisitos de Identificación y autenticación.

FIA_UID.2 Identificación de usuario antes de cualquier acción / OPERADORES

135 Jerárquico a: FIA_UID.1 Momento de la identificación

136 Dependencias: no existen dependencias.

137 FIA_UID.2.1 La TSF requerirá que cada usuario se identifique con éxito antes de permitirle cualquier acción en la que intervenga la TSF en nombre de ese usuario.

FIA_UAU.2 Autenticación de usuario antes de cualquier acción / OPERADORES

138 Jerárquico a: FIA_UAU.1 Momento de la autenticación

139 Dependencias: FIA_UID.1 Momento de la identificación

140 FIA_UAU.2.1 La TSF deberá requerir que cada usuario se autentique con éxito antes de permitirle cualquier acción en la que intervenga la TSF en nombre de ese usuario.

FIA_AFL.1 Manejo de fallos de autenticación / CLIENTES

141 Jerárquico a: No hay otros componentes.

142 Dependencias: FIA_UAU.1 Momento de la autenticación

143 FIA_AFL.1.1 La TSF deberá detectar cuando se producen [3] intentos de autenticación sin éxito relativos a [operadores intentando autenticarse con usuario/contraseña].

144 FIA_AFL.1.2 Cuando el número definido de intentos de autenticación sin éxito haya sido [alcanzado], la TSF deberá [bloquear la cuenta del operador e informar al responsable de seguridad ver FOM_PSN.2.1].

Requisitos de protección de datos de usuario

FDP_ACC.2 Control de acceso completo /OPERADORES

145 Jerárquico a: FDP_ACC.1 Subconjunto del control de acceso

146 Dependencias: FDP_ACF.1 Atributo de seguridad basado en el control de acceso

147 FDP_ACC.2.1 La TSF deberá hacer cumplir la [política de control de acceso de operadores] en [

- Sujetos: operadores;
- Objetos: fichero apuestas; ficheros clientes; servicios de administración de seguridad de la aplicación]

y para todas las operaciones entre sujetos y objetos cubiertas por la SFP.

148 FDP_ACC.2.2 La TSF deberá asegurar que todas las operaciones entre sujetos controlados por la TSF y cualquier objeto controlado por la TSF están cubiertos por el control de acceso de la SFP.

149 **Nota de aplicación:**

- Los servicios de administración de seguridad de la aplicación se corresponden, entre otros, con la validación de apuestas y gestión de riesgos, administrador de operarios, etc…

FDP_ACF.1 Control de acceso basado en atributos de seguridad /OPERADORES

150 Jerárquico a: No hay otros componentes.

151 Dependencias:

152 FDP_ACC.1 Subconjunto del control de acceso

153 FMT_MSA.3 Inicialización de atributos estática

154 FDP_ACF.1.1 La TSF deberá hacer cumplir la [política de control de acceso de operadores] a objetos basada en: [

- Sujetos: operadores; atributos: identidad del operador y su role asociado;
- Objetos:
  - fichero apuestas; sin atributos;
  - ficheros clientes; sin atributos;
  - servicios de administración de seguridad de la aplicación; sin atributos;]

155 FDP_ACF.1.2 La TSF deberá hacer cumplir las siguientes reglas para determinar si una operación entre sujetos controlados y objetos controlados es permitida: [se concederá acceso si el operador tiene los permisos necesarios para acceder a la funcionalidad de gestión de las apuestas (fichero

de apuestas), a la administración de clientes (fichero de clientes) y a la funcionalidad de administración de seguridad de la aplicación].

156 FDP_ACF.1.3 La TSF deberá autorizar explícitamente el acceso de sujetos a objetos basado en las siguientes reglas adicionales: [asignación: reglas, basadas en los atributos de seguridad, que explícitamente autorizna el acceso de sujetos a objetos].

157 FDP_ACF.1.4 La TSF deberá denegar explícitamente el acceso de sujetos a objetos basado en las siguientes reglas adicionales: [asignación: reglas, basadas en los atributos de seguridad, que explícitamente deniegan el acceso de sujetos a objetos].

FMT_MSA.1 Gestión de los atributos de seguridad /OPERADORES

158 Jerárquico a: No hay otros componentes.

159 Dependencias:

160 FDP_ACC.1 Subconjunto del control de acceso,

161 FMT_SMR.1 Roles de seguridad

162 FMT_SMF.1 Especificación de las Funciones de Gestión

163 Refinamiento:

164 FMT_MSA.1.1 La TSF deberá hacer cumplir la [política de control de acceso de operadores] para restringir la posibilidad de [selección: cambio_pordefecto, consulta, modificación, borrado, [asignación: otras operaciones]] los atributos de seguridad [asignación: lista de atributos de seguridad] to [administrador, selección: los roles identificados autorizados].

FMT_MSA.3 Inicialización de atributos estática /OPERADORES

165 Jerárquico a: No hay otros componentes.

166 Dependencias:

167 FMT_MSA.1 Gestión de los atributos de seguridad

168 FMT_SMR.1 Roles de seguridad

169 Refinamiento:

170 FMT_MSA.3.1 La TSF deberá hacer cumplir la [política de control de acceso de operadores] para proporcionar [selección, escoger uno: restrictivo, permisivo, [asignación: otra propriedad]] valores por defecto para los atributos de seguridad que se usan para hacer cumplir la SFP.

171 FMT_MSA.3.2 La TSF deberá permitir al [administrador, selección: los roles identificados autorizados] especificar valores iniciales alternativos para sobrescribir los valores por defecto cuando se crea un objeto o información.

FMT_SMR.1 Roles de seguridad/OPERADORES

172 Jerárquico a: No hay otros componentes.

173 Dependencias: FIA_UID.1 Timing de identificación

174 Refinamiento:

175 FMT_SMR.1.1 La TSF deberá mantener los roles [administrador, operario, selección: los roles identificados autorizados].

176 FMT_SMR.1.2 La TSF deberá ser capaz de asociar usuarios con roles.

177 **Nota de aplicación:**

- Cada usuario tiene asociado un rol a partir del cual se ejercita la política de control de acceso. Cuando se crea el usuario, el administrador le asigna el rol. El operario realiza las funciones de gestión de apuestas y clientes. El administrador realiza tareas de administración de seguridad del sistema completo (gestión de usuarios, comunicaciones, etc.).

Funciones de gestión de la seguridad

FMT_SMF.1 Especificación de las Funciones de Gestión /OPERADORES

178 Jerárquico a: No hay otros componentes.

179 Dependencias: no existen dependencias.

180 FMT_SMF.1.1 La TSF deberá ser capaz de realizar las siguientes funciones de gestión: [

- gestión de operadores;
- gestión de clientes
- administración de seguridad;
- asignación: *lista de funciones de gestión que serán proporcionadas por la TSF*].

181 **Nota de aplicación:**

- La función de gestión de operadores incluye la asignación del role a un usuario recién creado. Se mantendrán los roles de operario y administrador.

Funciones criptográficas

Integridad, no repudio de las Apuestas y Boletos

No Repudio en las apuestas realizadas por los Clientes:

182 **Nota de aplicación:**

- Un sistema que cumpla con este perfil de protección podrá optar por dos opciones:

OPCIÓN (I)

El cliente es el responsable de realizar un hash de la apuesta y firmarlo con su clave privada. El requisito para el cliente sería implementar un mecanismo de firma con RSA longitudes clave de 1024 bits, 2048 bits. El sistema deberá verificar la firma de la apuesta realizada por el cliente. El sistema importa el certificado del cliente (**FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS**) y verifica la firma.

FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS

183 Jerárquico a: No hay otros componentes.

184 Dependencias:

185 FDP_ACC.1 Subconjunto del control de acceso

186 FMT_MSA.3 Inicialización de atributos estática

187 Refinamiento:

188 FDP_ITC.1.1 La TSF deberá hacer cumplir la [política de control de acceso de operadores] durante la importación de datos de usuario, controlados por la SFP, de fuera del STOE.

189 FDP_ITC.1.2 La TSF deberá ignorar cualquiera de los atributos de seguridad asociados con los datos de usuario durante la importación de fuera del STOE.

190 FDP_ITC.1.3 La TSF deberá hacer cumplir las siguientes reglas durante la importación de datos de usuario controlados por la SFP de fuera del STOE: [asignación: reglas de control de importación adicionales].

OPCIÓN (II)

El sistema proporciona al cliente una aplicación de firma que calcula el hash y realiza la firma. Para ello, el sistema tendrá que generar el par de claves y pasarle la clave privada del certificado al cliente, para que éste pueda realizar la firma. No será necesario el requisito de importación de la clave pública ya que se dispondrá de ella y se deberán incluir requisitos de generación de las claves (**FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA**) y de la realización de las operaciones criptográficas (**FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS**):

FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA

191 Jerárquico a: No hay otros componentes.

192 Dependencias:

193 FCS_COP.1 Operación criptográfica

194 FCS_CKM.4 Destrucción de claves criptográficas

195 Refinamiento:

196 FCS_CKM.1.1 La TSF deberá generar claves criptográficas de acuerdo a un algoritmo específico de generación de claves criptográficas [RSA] y tamaños de claves criptográficas especificados [selección: 1024 bits, 2048 bits] que cumplan: [asignación: lista de estándares].

FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS

197 Jerárquico a: No hay otros componentes.

198 Dependencias:

199 FCS_CKM.1 Generación de claves criptográficas

200 FCS_CKM.4 Destrucción de claves criptográficas

201 Refinamiento:

202 FCS_COP.1.1 La TSF deberá realizar [CREAR RESUMEN DE LA APUESTA A SER FIRMADA] de acuerdo a un algoritmo criptográfico especificado [selección: SHA-224, SHA-256, SHA-384, SHA-512] y tamaños de resumen de mensaje [selección: 224, 256, 384, 512] que cumplan: [asignación: lista de estándares].

FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS

203 Jerárquico a: No hay otros componentes.

204 Dependencias:

205 FCS_CKM.1 Generación de claves criptográficas

206 FCS_CKM.4 Destrucción de claves criptográficas

207 Refinamiento:

208 FCS_COP.1.1 La TSF deberá realizar [FIRMAR LAS APUESTAS DEL CLIENTE] de acuerdo a un algoritmo criptográfico especificado [RSA] y tamaños de claves criptográficas [selección: 1024 bits, 2048 bits] que cumplan: [asignación: lista de estándares].

209 **Nota de aplicación:**

- Con independencia de la OPCIÓN elegida, el sistema deberá verificar el HASH y verificar la firma de las apuestas.

FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS

210 Jerárquico a: No hay otros componentes.

211 Dependencias:

212 FCS_CKM.1 Generación de claves criptográficas

213 FCS_CKM.4 Destrucción de claves criptográficas

214 Refinamiento:

215 FCS_COP.1.1 La TSF deberá realizar [VERIFICACIÓN DEL RESUMEN DE LA APUESTA] de acuerdo a un algoritmo criptográfico especificado [selección: SHA-224, SHA-256, SHA-384, SHA-512] y tamaños de resumen de mensaje [selección: 224, 256, 384, 512] que cumplan: [asignación: lista de estándares].

FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS

216 Jerárquico a: No hay otros componentes.

217 Dependencias:

218 FCS_CKM.1 Generación de claves criptográficas

219 FCS_CKM.4 Destrucción de claves criptográficas

220 Refinamiento:

221 FCS_COP.1.1 La TSF deberá realizar [VERIFICACIÓN DE FIRMA DE LAS APUESTAS DEL CLIENTE] de acuerdo a un algoritmo criptográfico especificado [RSA] y tamaños de claves criptográficas [selección: 1024 bits, 2048 bits] que cumplan: [asignación: lista de estándares].

222 **Nota de aplicación:**

- Verificación de la apuesta del cliente. El sistema verificará la firma realizada por el cliente (FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS) y verificará el hash asociado (FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS).
- No es necesario que el sistema borre la clave pública del cliente una vez verificada la firma, por lo que no es necesario que se satisfaga la dependencia de FCS_CKM.4 Destrucción de claves criptográficas.

FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS

223 Jerárquico a: No hay otros componentes.

224 Dependencias: no existen dependencias.

225 FDP_SDI.1.1 La TSF deberá monitorizar los datos de usuario almacenados en lugares controlados por la TSF para [errores de integridad en las apuestas] en todos los objetos, basándose en los siguientes atributos [asignación: atributos de datos de usuario].

226 **Nota de aplicación:**

- Estos requisitos tienen como objetivo mantener la integridad y no repudio de las apuestas en el servidor.
- **Garantía de integridad en el servidor.** El sistema deberá garantizar ante los clientes la integridad de sus apuestas que han sido validadas y que se almacenan en el sistema (**FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS**).

FCS_CKM.1 Generación de claves criptográficas / FIRMA DEL BOLETO

227 Jerárquico a: No hay otros componentes.

228 Dependencias:

229 FCS_COP.1 Operación criptográfica

230 FCS_CKM.4 Destrucción de claves criptográficas

231 Refinamiento:

232 FCS_CKM.1.1 La TSF deberá generar claves criptográficas de acuerdo a un algoritmo específico de generación de claves criptográficas [RSA] y tamaños de claves criptográficas especificados [selección: 1024 bits, 2048 bits] que cumplan: [asignación: lista de estándares].

FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO

233 Jerárquico a: No hay otros componentes.

234 Dependencias:

235 FCS_CKM.1 Generación de claves criptográficas

236 FCS_CKM.4 Destrucción de claves criptográficas

237 Refinamiento:

238 FCS_COP.1.1 La TSF deberá realizar [FIRMA DEL BOLETO] de acuerdo a un algoritmo criptográfico especificado [RSA] y tamaños de claves criptográficas [selección: 1024 bits, 2048 bits] que cumplan: [asignación: lista de estándares].

239 **Nota de aplicación:**

- Todas las apuestas formalizadas tienen asociado un boleto electrónico que se entrega como justificante al usuario, y que debe permitir garantizar la validez de la apuesta y su integridad, así como el no repudio de la misma por parte del sistema (la firma electrónica de la apuesta por parte del cliente garantiza el no repudio de la apuesta por parte de cliente). El sistema deberá firmar electrónicamente el boleto con un certificado emitido por la entidad.

- No es necesario que el sistema borre su clave una vez realizada la firma, por lo que no es necesario que se satisfaga la dependencia de FCS_CKM.4 Destrucción de claves criptográficas.

Establecimiento de criterios de aleatoriedad en aquellas apuestas en que así se precise

FCS_RNG.1 Generación de números aleatorios

240 Jerárquico a: No hay otros componentes.

241 Dependencias: No hay dependencias

242 FCS_RNG.1.1 La TSF deberá proporcionar un generador de números aleatorios [selección: determinístico, no-determinístico] que cumpla [asignación: lista de características de seguridad].

243 FCS_RNG.1.2 La TSF deberá proporcionar un generador de números aleatorios que cumpla [asignación: una métrica de cualidad definida].

244 **Nota de aplicación:**

- Se requiere que se satisfagan los criterios de aleatoriedad en aquellas apuestas en las que así se precise (se seleccionará este requisito si las apuestas precisan la generación de número aleatorios, como por ejemplo, los sistemas de lotería). La generación de los datos se realizará de forma aleatoria e imprevisible, tal y como se requiere en [RACC]. La selección del primer componente se refiere a la tipología de RNGs definida por el NIST en la norma FIPS 140-2.

Comunicaciones

Comunicaciones con los CLIENTES u otras entidades externas

FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES

245 Jerárquico a: No hay otros componentes.

246 Dependencias: no existen dependencias.

247 Refinamiento:

248 FTP_ITC.1.1 La TSF deberá proporcionar un canal de comunicación entre ella y otro producto de las TI seguro que sea lógicamente distinto de otros canales de comunicación y proporcione identificación asegurada en sus puntos finales, además de protección de los datos del canal contra modificación o revelación.

249 FTP_ITC.1.2 La TSF deberá permitir [clientes, selección: otras entidades externas]] iniciar la comunicación a través del canal seguro.

250 FTP_ITC.1.3 La TSF deberá iniciar la comunicación a través del canal seguro para [funcionalidad del cliente, selección: otras operaciones de otras entidades externas].

251 **Nota de aplicación:**

- Se requiere un canal seguro en las comunicaciones con los clientes para la realización de todos los servicios que le ofrece el sistema, tales como la realización de las apuestas, funcionales de gestión de seguridad (cambio de contraseña), actualizar sus datos personales, recarga de saldo, solicitud de reintegro, etc. Otras entidades externas que podrían requerir canal seguro

son: la Consejería de la Comunidad Autónoma correspondiente o las entidades que proporcionen información sobre los mercados. En casos, la declaración de seguridad del sistema deberá incluirlos en la operación de selección del segundo componente o iterar el requisito para cada entidad externa.

Comunicaciones con las Máquinas de apuestas

FTP_ITC.1 Canal seguro Inter-TSF / MÁQUINAS DE APUESTAS

252 Jerárquico a: No hay otros componentes.

253 Dependencias: no existen dependencias.

254 Refinamiento:

255 FTP_ITC.1.1 La TSF deberá proporcionar un canal de comunicación entre ella y otro producto de las TI seguro que sea lógicamente distinto de otros canales de comunicación y proporcione identificación asegurada en sus puntos finales, además de protección de los datos del canal contra modificación o revelación.

256 FTP_ITC.1.2 La TSF deberá permitir [máquina de apuestas] iniciar la comunicación a través del canal seguro.

257 FTP_ITC.1.3 La TSF deberá iniciar la comunicación a través del canal seguro para [establecer su identidad, selección: otras operaciones].

258 **Nota de aplicación:**

- En el caso de que la entidad del dominio CLIENTES se corresponda con una "máquina de apuestas" (ver descripción del dominio CLIENTES), el certificado usado en el establecimiento del canal seguro de comunicación con la unidad central, será un certificado reconocido (conforme a la Ley 59/2003, de Firma Electrónica) y cuya expedición corresponderá al órgano competente, que podrá externalizar este servicio en un Prestador de Servicios de Certificación.. La revocación del certificado implicará que la máquina que aloje el dispositivo de creación de firma asociado no podrá prestar sus servicios.

Auditoría

FAU_GEN.1 Generación de datos de auditoría / OPERADORES

259 Jerárquico a: No hay otros componentes.

260 Dependencias: FPT_STM.1 Sellados de tiempo confiables

261 FAU_GEN.1.1 La TSF deberá ser capaz de generar un registro de auditoría de los siguientes eventos auditables:

a) Inicio y finalización de las funciones de auditoría;

b) Todos los eventos auditables para el [sin especificar] nivel de auditoría; y

c) [actividades de gestión de seguridad de la aplicación, apuestas validadas, asignación: otros eventos auditables definidos específicamente].

262 FAU_GEN.1.2 La TSF deberá registrar dentro de cada registro de auditoría al menos la siguiente información:

a) fecha y hora del evento, tipo de evento, identidad del sujeto (si es aplicable), y el resultado (éxito o fallo) del evento; y

b) Para cada tipo de evento, basado en las definiciones de eventos auditables de los componentes funcionales incluidos en el PP/DS, [asignación: otra información relevante de auditoría].

FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES

263 Jerárquico a: No hay otros componentes.

264 Dependencias: Generación de datos de auditoría / OPERADORES

265 FAU_STG.1.1 La TSF deberá proteger los registros de auditoria almacenados en la traza de auditoría contra el borrado no autorizado.

266 FAU_STG.1.2 La TSF deberá ser capaz de [selección, elegir uno de: evitar, detectar] modificaciones no autorizadas de los registros almacenados de la traza de auditoría.

REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL

267 No existen requisitos de control operacional en el dominio OPERADORES INTERNOS adicionales a los especificados en la sección de requisitos operacionales comunes a los tres dominios.

Dominio SOPORTE

REQUISITOS FUNCIONALES TÉCNICOS

Requisitos de Identificación y autenticación.

FIA_UID.2 Identificación de usuario antes de cualquier acción / SOPORTE

268 Jerárquico a: FIA_UID.1 Momento de la identificación

269 Dependencias: no existen dependencias.

270 FIA_UID.2.1 La TSF requerirá que cada usuario se identifique con éxito antes de permitirle cualquier acción en la que intervenga la TSF en nombre de ese usuario.

FIA_UAU.2 Autenticación de usuario antes de cualquier acción / SOPORTE

271 Jerárquico a: FIA_UAU.1 Momento de la autenticación

272 Dependencias: FIA_UID.1 Momento de la identificación

273 FIA_UAU.2.1 La TSF deberá requerir que cada usuario se autentique con éxito antes de permitirle cualquier acción en la que intervenga la TSF en nombre de ese usuario.

FIA_AFL.1 Manejo de fallos de autenticación / SOPORTE

274 Jerárquico a: No hay otros componentes.

275 Dependencias: FIA_UAU.1 Momento de la autenticación

276 FIA_AFL.1.1 La TSF deberá detectar cuando se producen [3] intentos de autenticación sin éxito relativos a [usuarios de soporte intentando autenticarse con usuario/contraseña].

277 FIA_AFL.1.2 Cuando el número definido de intentos de autenticación sin éxito haya sido [alcanzado], la TSF deberá [bloquear la cuenta del operador e informar al responsable de seguridad ver FOM_PSN.2.1].

Requisitos de protección de datos de usuario. Política de control de acceso

FDP_ACC.2 Control de acceso completo / SOPORTE

278 Jerárquico a: FDP_ACC.1 Subconjunto del control de acceso

279 Dependencias: FDP_ACF.1 Atributo de seguridad basado en el control de acceso

280 FDP_ACC.2.1 La TSF deberá hacer cumplir la [política de control de acceso de soporte] en [

- Sujetos: usuarios de soporte;
- Objetos: configuración de seguridad de los componentes de soporte]

y para todas las operaciones entre sujetos y objetos cubiertas por la SFP.

281 FDP_ACC.2.2 La TSF deberá asegurar que todas las operaciones entre sujetos controlados por la TSF y cualquier objeto controlado por la TSF están cubiertos por el control de acceso de la SFP.

282 **Nota de aplicación:**

- Se denomina usuario de soporte, al usuario que realiza las funciones de administración y mantenimiento de los componentes que dan soporte a la aplicación de formalización de apuestas, con el rol que tenga asignado.

FDP_ACF.1 Atributo de seguridad basado en el control de acceso / SOPORTE

283 Jerárquico a: No hay otros componentes.

284 Dependencias:

285 FDP_ACC.1 Subconjunto del control de acceso

286 FMT_MSA.3 Inicialización de atributos estática

287 FDP_ACF.1.1 La TSF deberá hacer cumplir la [política de control de acceso de soporte] a objetos basada en: [

- Sujetos: usuarios de soporte; atributos: identidad del usuario y su role asociado;
- Objetos: servicios de administración de seguridad; sin atributos;]

288 FDP_ACF.1.2 La TSF deberá hacer cumplir las siguientes reglas para determinar si una operación entre sujetos controlados y objetos controlados

es permitida: [se concederá acceso si el usuario de soporte tiene los permisos necesarios para acceder a la funcionalidad de administración de seguridad].

289 FDP_ACF.1.3 La TSF deberá autorizar explícitamente el acceso de sujetos a objetos basado en las siguientes reglas adicionales: [asignación: reglas, basadas en los atributos de seguridad, que explícitamente autorizan el acceso de sujetos a objetos].

290 FDP_ACF.1.4 La TSF deberá denegar explícitamente el acceso de sujetos a objetos basado en las siguientes reglas adicionales: [asignación: reglas, basadas en los atributos de seguridad, que explícitamente deniegan el acceso de sujetos a objetos].

FMT_MSA.1 Gestión de los atributos de seguridad / SOPORTE

291 Jerárquico a: No hay otros componentes.

292 Dependencias:

293 FDP_ACC.1 Subconjunto del control de acceso,

294 FMT_SMR.1 Roles de seguridad

295 FMT_SMF.1 Especificación de las Funciones de Gestión

296 Refinamiento:

297 FMT_MSA.1.1 La TSF deberá hacer cumplir la [política de control de acceso de soporte] para restringir la posibilidad de [selección: cambio_pordefecto, consulta, modificación, borrado, [asignación: otras operaciones]] los atributos de seguridad [asignación: lista de atributos de seguridad] to [administrador, selección: los roles identificados autorizados].

FMT_MSA.3 Inicialización de atributos estática / SOPORTE

298 Jerárquico a: No hay otros componentes.

299 Dependencias:

300 FMT_MSA.1 Gestión de los atributos de seguridad

301 FMT_SMR.1 Roles de seguridad

302 Refinamiento:

303 FMT_MSA.3.1 La TSF deberá hacer cumplir la [política de control de acceso de soporte] para proporcionar [selección, escoger uno: restrictivo, permisivo, [asignación: otra propiedad]] valores por defecto para los atributos de seguridad que se usan para reforzar la SFP.

304 FMT_MSA.3.2 La TSF deberá permitir al [administrador de soporte, selección: los roles identificados autorizados] especificar valores iniciales alternativos para sobrescribir los valores por defecto cuando se crea un objeto o información.

FMT_SMR.1 Roles de seguridad/OPERADORES

305 Jerárquico a: No hay otros componentes.

306 Dependencias: FIA_UID.1 Timing de identificación

307 Refinamiento:

308 FMT_SMR.1.1 La TSF deberá mantener los roles [administrador de soporte, selección: los roles identificados autorizados].

309 FMT_SMR.1.2 La TSF deberá ser capaz de asociar usuarios con roles.

310 **Nota de aplicación:**

- Cada usuario tiene asociado un rol a partir del cual se ejercita la política de control de acceso. Cuando se crea el usuario, el administrador le asigna el rol.

Funciones de gestión de la seguridad

FMT_SMF.1 Especificación de las Funciones de Gestión / SOPORTE

311 Jerárquico a: No hay otros componentes.

312 Dependencias: no existen dependencias.

313 FMT_SMF.1.1 La TSF deberá ser capaz de realizar las siguientes funciones de gestión: [

- gestión de usuarios de soporte;
- gestión de red;
- administración del sistema operativo;
- administración de BD;
- configuración de cortafuegos;
- configuración IDS;
- gestión de copias de respaldo y restauración;
- asignación: lista de funciones de gestión que serán proporcionadas por la TSF].

314 **Nota de aplicación:**

- La función de gestión de usuarios incluye la asignación del role a un usuario recién creado.

Tolerancia a fallos y recuperación

FRU_FLT.2 Tolerancia a fallos limitada

315 Jerárquico a: FRU_FLT.1 Tolerancia a fallos degradada

316 Dependencias: FPT_FLS.1 Fallo con preservación de estado seguro

317 Refinamiento:

318 FRU_FLT.2.1 La SSF deberá asegurar la operación de todas las funcionalidades del STOE cuando ocurran los siguientes fallos: [

- Fallo del sistema por pérdida de suministro eléctrico.
- Fallo simple del sistema
- Robo
- Incendio
- asignación: otros tipos de fallos].

FPT_RCV.2 Recuperación automática

319 Refinamiento:

320 Jerárquico a: FPT_RCV.1 Recuperación manual

321 Dependencias: AOD_OGD.2 Verificación del uso de las SSFs en el manual de usuario

322 FPT_RCV.2.1 Cuando la recuperación automática desde [

- Fallo del sistema por pérdida de suministro eléctrico
- Fallo simple del sistema
- Robo
- Incendio
- asignación: otros tipos de fallos]

no es posible, la SSF deberá entrar en modo de mantenimiento proporcionando la posibilidad de volver a un estado seguro sin pérdida de transacciones y garantizando una disponibilidad del servicio del 99'96 % (máximo 15 min. al mes de caida).

323 FPT_RCV.2.2 Para [

- Fallo simple del sistema por pérdida de suministro eléctrico
- asignación: otros tipos de fallos],

la TSF deberá asegurar la vuelta del STOE a un estado seguro utilizando procedimientos automatizados que garanticen la inexistencia de pérdida de transacciones y garantizando una disponibilidad del servicio del 99'96 % (máximo 15 min. al mes de caida).

324 **Nota de aplicación:**

- Estos requisitos tienen como objetivo mantener las garantías de las apuestas en el caso de robo, incendio, pérdida de suministro eléctrico o fallo simple del sistema. Para ello se deberá disponer de un sistema de respaldo que permita restablecer el estado del sistema y las evidencias generadas por los mecanismos de seguridad que garantizan el no repudio e integridad de las apuestas realizadas **sin pérdida de transacciones** y **garantizando una disponibilidad del servicio del 99'96 % (máximo 15 min. al mes de caida)**.

- Se ha sustituido la dependencia AGD_OPE.1 de evaluación de productos, por AOD_OGD.2 Verificación del uso de las SSFs en el manual de usuario, perteneciente a evaluación de sistemas.

Funciones criptográficas

Cifrado de los discos de los servidores

FCS_CKM.1 Generación de claves criptográficas / CIFRADO DE DISCOS

325 Jerárquico a: No hay otros componentes.

326 Dependencias:

327 FCS_COP.1 Operación criptográfica

328 FCS_CKM.4 Destrucción de claves criptográficas

329 Refinamiento:

330 FCS_CKM.1.1 La TSF deberá obtener claves criptográficas de acuerdo a un algoritmo específico de generación de claves criptográficas [algoritmo de obtención de la clave AES basada en un factor de autorización externo] y tamaños de claves criptográficas especificados [selección: 128 bits, 256 bits] que cumplan: [asignación: lista de estándares].

FCS_CKM.4 Destrucción de claves criptográficas / CIFRADO DE DISCOS

331 Jerárquico a: No hay otros componentes.

332 Dependencias: FCS_CKM.1 Generación de claves criptográficas

333 FCS_CKM.4.1 La TSF deberá destruir las claves criptográficas de acuerdo a un método específico de destrucción de claves criptográficas [zeroización de la clave] que cumpla: [asignación: lista de estándares].

FCS_COP.1 Operación criptográfica / CIFRADO DE DISCOS

334 Jerárquico a: No hay otros componentes.

335 Dependencias:

336 FCS_CKM.1 Generación de claves criptográficas

337 FCS_CKM.4 Destrucción de claves criptográficas

338 Refinamiento:

339 FCS_COP.1.1 La TSF deberá realizar [CIFRADO/DESCIFRADO DE LOS SISTEMAS DE FICHEROS DE LOS SERVIDORES] de acuerdo a un algoritmo criptográfico especificado [AES operando en alguno de los siguientes modos: selección: CBC, CCM, CFB, CTR, OFB, XTS] y tamaños de claves criptográficas [selección: 128 bits, 256 bits] que cumplan: [asignación: lista de estándares].

340 **Nota de aplicación:**

- Estos requisitos tienen como objetivo mantener la confidencialidad de los datos de carácter personal y apuestas de los CLIENTES (y demás información almacenada en los discos). Para ello se requiere que los sistemas de ficheros de los servidores estén cifrados con AES en alguno de los modos que se indican en la selección y tamaños de claves indicados. Los servidores no podrán arrancarse sin introducir una "passphrase" o factor de autorización externo. La clave de cifrado se obtendrá (**FCS_CKM.1 Generación de claves criptográficas / CIFRADO DE DISCOS**) a partir de este factor de autorización que introduce el usuario antes de arrancar.

Cifrado de los BACKUPS

FCS_CKM.1 Generación de claves criptográficas / CIFRADO DE BACKUPS

341 Jerárquico a: No hay otros componentes.

342 Dependencias:

343 FCS_COP.1 Operación criptográfica

344 FCS_CKM.4 Destrucción de claves criptográficas

345 Refinamiento:

346 FCS_CKM.1.1 La SSF deberá generar claves criptográficas de acuerdo a un algoritmo específico de generación de claves criptográficas [generación de claves AES] y tamaños de claves criptográficas especificados [selección: 128 bits, 256 bits] que cumplan: [asignación: lista de estándares].

FCS_CKM.4 Destrucción de claves criptográficas / CIFRADO DE BACKUPS

347 Jerárquico a: No hay otros componentes.

348 Dependencias: FCS_CKM.1 Generación de claves criptográficas

349 Refinamiento:

350 FCS_CKM.4.1 La SSF deberá destruir las claves criptográficas de acuerdo a un método específico de destrucción de claves criptográficas [zeroización de la clave] que cumpla: [asignación: lista de estándares].

FCS_COP.1 Operación criptográfica / CIFRADO DE BACKUPS

351 Jerárquico a: No hay otros componentes.

352 Dependencias:

353 FCS_CKM.1 Generación de claves criptográficas

354 FCS_CKM.4 Destrucción de claves criptográficas

355 Refinamiento:

356 FCS_COP.1.1 La SSF deberá realizar [CIFRADO/DESCIFRADO DE BACKUPS] de acuerdo a un algoritmo criptográfico especificado [AES operando en alguno de los siguientes modos: selección: CBC, CCM, CFB, CTR, OFB, XTS] y tamaños de claves criptográficas [selección: 128 bits, 256 bits] que cumplan: [asignación: lista de estándares].

357 **Nota de aplicación:**

- Estos requisitos tienen como objetivo mantener la confidencialidad de los datos de carácter personal y apuestas de los CLIENTES almacenados en las copias de respaldo. Para ello se requiere que el contenido de las copias esté cifrado con AES en alguno de los modos que se indican en la selección y tamaños de claves indicados.

Borrado seguro de Backups

FDP_RIP.1 Protección de un subconjunto de la información residual / BACKUPS

358 Jerárquico a: No hay otros componentes.

359 Dependencias: no existen dependencias.

360 FDP_RIP.1.1 La TSF deberá asegurar que cualquier información previa contenida en un recurso no esté disponible a partir de la [desasignación del recurso] para los siguientes objetos: [Backups o copias de seguridad].

361 **Nota de aplicación:**

- Cuando un soporte o copia de seguridad vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él.

Fuente de tiempo

FPT_STM.1 Sellados de tiempo fiables

362 Jerárquico a: No hay otros componentes.

363 Dependencias: no existen dependencias.

364 FPT_STM.1.1 La TSF deberá de ser capaz de proporcionar sellados de tiempo fiables.

365 **Nota de aplicación:**

- Es importante garantizar la fiabilidad de las marcas de tiempo utilizadas en la generación de auditoría de los tres dominios y la fiabilidad de las marcas de tiempo que se asocian a las apuestas. Se asignarán los sellos de tiempo a las apuestas formalizadas por los clientes y a los eventos de auditoría.

Auditoría y Detección de Intrusos

FAU_GEN.1 Generación de datos de auditoría / SOPORTE

366 Jerárquico a: No hay otros componentes.

367 Dependencias: FPT_STM.1 Sellados de tiempo fiables

368 FAU_GEN.1.1 La TSF deberá ser capaz de generar un registro de auditoría de los siguientes eventos auditables:

a) Inicio y finalización de las funciones de auditoría;

b) Todos los eventos auditables para el [sin especificar] nivel de auditoría; y

c) [actividades de gestión de seguridad, eventos de seguridad necesarios para la detección de intrusos en el firewall, asignación: otros eventos auditables definidos específicamente].

369 FAU_GEN.1.2 La TSF deberá registrar dentro de cada registro de auditoría al menos la siguiente información:

a) fecha y hora del evento, tipo de evento, identidad del sujeto (si es aplicable), y el resultado (éxito o fallo) del evento; y

b) Para cada tipo de evento, basado en las definiciones de eventos auditables de los componentes funcionales incluidos en el PP/DS, [asignación: otra información relevante de auditoría].

FAU_STG.1 Protección de la traza de auditoría almacenada / SOPORTE

370 Jerárquico a: No hay otros componentes.

371 Dependencias: Generación de datos de auditoría / SOPORTE

372 FAU_STG.1.1 La TSF deberá proteger los registros de auditoria almacenados en la traza de auditoría contra el borrado no autorizado.

373 FAU_STG.1.2 La TSF deberá ser capaz de [selección, elegir uno de: evitar, detectar] modificaciones no autorizadas de los registros almacenados de la traza de auditoría.

FAU_SAA.1 Análisis de violaciones potenciales

374 Jerárquico a: No hay otros componentes.

375 Dependencias: FAU_GEN.1 Generación de datos de auditoría

376 SAU_SAA.1.1 La TSF deberá ser capaz de aplicar un conjunto de reglas durante la monitorización de los eventos de auditoría y basándose en estas reglas indicar una violación potencial de la ejecución de los SFRs.

377 FAU_SAA.1.2 La TSF deberá hacer cumplir las siguientes reglas para monitorizar los eventos auditados:

a) Acumulación o combinación de [asignación: subconjunto de los eventos auditables definidos] subconjunto de los eventos auditables definidos;

b) [asignación: cualquier otra regla].

REQUISITOS FUNCIONALES DE CONTROL OPERACIONAL

Política de seguridad

FOD_POL.1 Política de seguridad

378 Dependencias: no existen dependencias.

379 FOD_POL.1.1 La OSF deberá definir [asignación: el compromiso de gestión] de que la gestión soportará activamente la seguridad dentro de la organización a través de una clara dirección, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.

380 FOD_POL.1.2 La OSF deberá definir [asignación: política de seguridad de la información] incluyendo metas, objetivos, ámbito, cumplimiento con la legislación, requisitos contractuales y estándares, análisis de riesgos y gestión de riesgos, educación en seguridad, formación, y requisitos de concienciación, gestión de la continuidad del negocio, consecuencias de las violaciones de la política de seguridad de la información y de las responsabilidades de la organización, además de su enfoque para gestionar la seguridad de la información.

381 FOD_POL.1.3 La OSF deberá definir [asignación: procedimientos formales] para las revisiones de gestión que incluyan como entrada los resultados de las revisiones de gestión previas, los cambios que pudieran afectar el enfoque de la organización para gestionar la información de seguridad, recomendaciones proporcionadas por autoridades relevantes, últimas amenazas y vulnerabilidades, e informes de incidentes de seguridad.

382 FOD_POL.1.4 La OSF deberá definir [asignación: política de personal] proporcionando una forma de que el personal reciba información de la violación de los controles operacionales.

383 FOD_POL.1.5 La OSF deberá definir [asignación: requisitos de seguridad] medios para comunicar la acción de una violación de los controles operacionales antes de que tenga lugar el acceso por parte del personal a los recursos del sistema.

384 FOD_POL.1.6 La OSF deberá definir [asignación: política de personal] que proporcione un medio para imponer sanciones, como por ejemplo multas, eliminación de privilegios, suspensión o cualquier otra sanción debido a la violación de los controles operacionales.

385 FOD_POL.1.7 La OSF deberá definir [asignación: requisitos de seguridad] que borren, limiten, u otra acción similar, a los recursos del sistema por parte del violador, hasta que se establezca el criterio para la reincorporación.

386 FOD_POL.1.8 La OSF deberá definir [asignación: política de personal] que proporcione una forma de cesar al personal que cometa una violación de las reglas y procedimientos, según lo permitido por la ley.

387 FOD_POL.1.9 La OSF deberá definir [asignación: requisitos de seguridad] para todos los requisitos estatutarios, regulatorios, y contractuales relevantes y bajo el enfoque de la organización, de forma que se cumplan estos requisitos y se mantengan actualizados para cada sistema de información y de organización.

388 FOD_POL.1.10 La OSF deberá definir [asignación: política de seguridad de la información] de forma que se desarrolle e implemente un conjunto apropiado de procedimientos para el etiquetado y manejo de la información de acuerdo con el esquema de clasificación adoptado por la organización.

389 FOD_POL.1.11 La OSF deberá definir [asignación: política de seguridad de la información] que asegure que el enfoque de la organización para manejar la seguridad de la información y su implementación (p.e. controles de los objetivos de control, políticas, procesos, y procedimientos para la seguridad de la información) se revisa independientemente de forma periódica, o cuando se producen cambios significativos relativos a la implementación de la seguridad.

390 FOD_POL.1.12 La OSF deberá definir [asignación: política de seguridad de la información] que asegure que todos los requisitos de seguridad identificados se tratan adecuadamente antes de dar a los usuarios acceso a la información o activos de la organización.

391 FOD_POL.1.13 La OSF deberá definir [asignación: política de seguridad de la información] que asegure que se aprueba un documento de política de seguridad de la información, y se publica y comunica a todos los empleados y partes relevantes externas.

392 **Nota de aplicación:**

- El fabricante deberá desarrollar un documento de política de seguridad de la información con el siguiente contenido:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos: apuestas y fichero de clientes. Política de protección y privacidad

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.

c) Funciones y obligaciones del personal (con filosofía de separación de funciones). Roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información. Deberá contener la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado. Deberán existir procedimientos para la resolución de conflictos entre dichos responsables. Se deberá definir un responsable de seguridad. Formación en seguridad.

d) Descripción detallada de las estructuras de datos que representa la información que se quiere proteger: ficheros de apuestas y clientes y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Gestión de soportes

g) Procedimientos de realización de copias de respaldo y de recuperación de los datos.

h) Mecanismos de registro y autenticación de clientes.

i) Garantías del servicio y las comunicaciones.

j) Ubicación de los sistemas de información que tratan los datos. Descripción de los mecanismos de seguridad física.

k) Auditoría: registro de acceso y eventos generales.

l) Plan de continuidad del negocio

FOD_POL.2 Protección de datos y política de privacidad

393 Dependencias: no existen dependencias.

394 FOD_POL.2.1 La OSF deberá desarrollar e implementar [asignación: protección de datos y política de privacidad].

395 **Nota de aplicación:**

- Se debe garantizar la confidencialidad, integridad y disponibilidad de las apuestas y datos de carácter personal de los clientes que se procesan en el sistema. Así mismo, se deberá proporcionar garantía de no repudio en origen de las apuestas.

Personal

FOD_PSN.1 Roles y responsabilidades del personal

396 Dependencias:

397 FOD_POL.1 Política de seguridad

398 FOD_RSM.1 Gestión de riesgos de la organización

399 FOD_PSN.1.1 La OSF deberá definir y documentar [asignación: roles y responsabilidades] de los empleados, contratistas y terceras partes de acuerdo a la política de seguridad de la información de la organización.

400 FOD_PSN.1.2 La OSF deberá definir [asignación: responsabilidades] para llevar a cabo la finalización del contrato de un empleado o bien un cambio de contrato.

401 FOD_PSN.1.3 La OSF deberá definir [asignación: requisitos de seguridad] para los requisitos de seguridad en curso, las responsabilidades legales, y acuerdos de confidencialidad en curso, los términos y condiciones definidos para un periodo de tiempo posterior a la finalización del contrato del empleado, del contratista o de una tercera parte y para la comunicación de las responsabilidades de salida.

402 FOD_PSN.1.4 La OSF deberá definir [asignación: requisitos de seguridad] para el personal que trabaje en áreas seguras.

403 FOD_PSN.1.5 La OSF deberá definir [asignación: requisitos de seguridad] que aseguren que los derechos de acceso de todos los empleados, contratistas y terceras partes a la información y a las instalaciones que procesan información deberán ser eliminados una vez finalizado el contrato o acuerdo, o bien cuando se produzca una modificación del mismo.

404 FOD_PSN.1.6 La OSF deberá definir [asignación: requisitos de seguridad] sobre todos los candidatos a personal, contratistas y terceras partes de acuerdo a las leyes y regulaciones oportunas.

405 FOD_PSN.1.7 La OSF deberá definir [asignación: procedimientos] que se desarrollen y se lleven a cabo cuando se reúnan y presenten evidencias con la finalidad de llevar a cabo alguna acción disciplinaria dentro de la organización.

406 FOD_PSN.1.8 La OSF deberá definir [asignación: requisitos de seguridad] en un proceso disciplinario formal para aquellos empleados, contratistas y terceras partes que estén involucrados en un problema de seguridad.

407 FOD_PSN.1.9 La OSF deberá definir [asignación: requisitos de seguridad] en los términos y condiciones del contrato que establezcan: las responsabilidades legales y derechos del empleado, contratista y terceras partes, las responsabilidades para la clasificación y gestión de los datos de la organización manejados por el empleado, contratista y terceras partes, las responsabilidades del empleador para el manejo de los datos de carácter personal, incluyendo aquellos creados como resultado, o en el curso, del trabajo dentro de la propia organización, las responsabilidades que van más allá de las instalaciones de la organización y fuera de las horas normales de trabajo y las acciones a llevar a cabo si el empleado, contratista o terceras partes no tienen en cuenta los requisitos de seguridad del empleador. Las responsabilidades contenidas dentro de los términos y condiciones del contrato del empleado deberán continuar por un periodo de tiempo definido después de la finalización del mismo.

408 FOD_PSN.1.10 La OSF deberá definir [asignación: reglas] respecto a las responsabilidades relativas a la seguridad de la información de los empleados, contratistas y terceras partes y que serán acordadas y firmadas como parte de sus obligaciones contractuales con la organización.

409 FOD_PSN.1.11 La OSF deberá definir [asignación: reglas] que contemplen la firma de acuerdos de confidencialidad y no revelación de información como parte de sus términos iniciales y condiciones de empleo antes de darles acceso a las instalaciones donde se procesa la información y que se identifiquen y revisen regularmente requisitos de confidencialidad y no revelación de información que reflejen las necesidades de la organización para la protección de la información.

410 FOD_PSN.1.12 La OSF deberá definir [asignación: requisitos de seguridad] para los acuerdos de confidencialidad cuando haya cambios en los términos del contrato, particularmente cuando haya empleados a punto de dejar la organización, o contratos que están a punto de finalizar.

411 FOD_PSN.1.13 La OSF deberá definir [asignación: reglas] de forma que todo el personal lleve alguna forma visible de identificación.

412 FOD_PSN.1.14 La OSF deberá definir [asignación: reglas] para que no se acceda a las instalaciones de la organización excepto cuando se autorice.

413 FOD_PSN.1.15 La OSF deberá definir [asignación: reglas] relativas al uso aceptable de la información y de los recursos de la organización.

414 **Nota de aplicación:**

- Los activos de la organización incluyen el sofware realizado previamente, documentos corporativos, dispositivos portátiles, tarjetas de crédito, tarjetas de acceso, software, manuales e información almacenada en medios electrónicos.

415 FOD_PSN.1.16 La OSF deberá definir [asignación: reglas] que especifiquen que todos los empleados, contratistas y terceras partes deberán devolver todos los activos de la organización en su posesión después de la terminación del contrato o acuerdo.

416 FOD_PSN.1.17 La OSF deberá definir [asignación: reglas] que contemplen que todos los empleados, contratistas y terceras partes no sacarán activos de la organización sin la correspondiente autorización.

417 FOD_PSN.1.18 La OSF deberá definir [asignación: reglas] que contemplen que las obligaciones y áreas de responsabilidad están segregadas de forma que se reduce la posibilidad de una modificación no autorizada o no intencionada, o bien el mal uso de los activos de la organización.

418 FOD_PSN.1.19 La OSF deberá definir [asignación: requisitos de seguridad] aplicables en un proceso disciplinario formal para aquellos empleados que involucrados en un problema de seguridad.

Gestión de riesgos

FOD_RSM.1 Gestión de riesgos de la organización

419 Dependencias: no existen dependencias.

420 FOD_RSM.1.1 La OSF deberá definir [asignación: procedimientos] para la gestión de riesgos que enumeren la información de la organización y las instalaciones dónde se procesa la información, incluyendo los trabajadores desde casa y otros usuarios remotos o desplazados.

421 FOD_RSM.1.2 La OSF deberá definir [asignación: requisitos de seguridad] para la realización de la gestión del riesgo al sistema operacional con el proceso de negocio.

422 FOD_RSM.1.3 La OSF deberá definir [asignación: requisitos de seguridad] que contemplen que se obtiene información periódica acerca de vulnerabilidades aplicables a los sistema de información, que la exposición de la organización a tales vulnerabilidades es evaluada, y que se llevan a cabo las correspondientes medidas para tratar el riesgo asociado.

Gestión de los activos

FOM_PRM.2 Segregación de privilegios

423 Dependencias: no existen dependencias.

424 FOM_PRM.2.1 La OSF deberá definir [asignación: reglas] que contemplen la segregación de privilegios para reducir la posibilidad de una modificación no autorizada o el mal uso de los activos, de forma que se lleve a cabo la separación de la inicialización de un evento de su autorización.

425 FOM_PRM.2.2 La OSF deberá definir [asignación: requisitos de seguridad] en la asignación de privilegios a identidades de usuario diferentes de aquellas que se utilizan normalmente para el negocio.

426 **Nota de aplicación:**

- Se deberá documentar las personas responsables de los datos de carácter personal y aquellas que tienen autorización de acceso a dichos datos. El derecho a acceso se implementará mediante las políticas de control de acceso definidas para los tres dominios (CLIENTES, OPERADORES INTERNOS y SOPORTE).

FOM_CLS.2 Identificación de Activos

427 Dependencias: No hay dependencias.

428 FOM_CLS.2.1 La OSF deberá definir [asignación: requisitos de seguridad] en la identificación, especificación del tipo de activo, la función del mismo, los requisitos de gestión, los niveles de protección adecuados con la importancia de los activos de acuerdo a su propietario y su clasificación de seguridad, y el registro de su localización actual en un inventario para cada activo.

429 FOM_CLS.2.2 La OSF deberá definir [asignación: requisitos de seguridad] en la elaboración y mantenimiento de un inventario con todos los activos importantes.

430 FOM_CLS.2.3 La OSF deberá definir [asignación: requisitos de seguridad] en el periodo de retención de información empresarial importante, y también algunos requisitos para copias que se mantendrán de forma permanente.

FOM_PSN.1 Propiedad de los activos

431 Dependencias: FOA_POL.3 Gestión de los activos de usuario

432 FOM_PSN.1.1 La OSF deberá definir [asignación: requisitos de seguridad] de forma que toda la información y los activos asociados con las instalaciones que procesan información son propiedad de una parte específica de la organización.

Gestión de la seguridad

FOM_PSN.2 Gestores de seguridad

433 Dependencias: no existen dependencias.

434 FOM_PSN.2.1 La OSF deberá definir [asignación: requisitos de seguridad] sobre la asignación de un responsable específico para cada control de seguridad.

435 FOM_PSN.2.2 La OSF deberá definir [asignación: requisitos de seguridad] de forma que la gestión requiera de los empleados, contratistas y terceras partes para aplicar la seguridad de acuerdo con políticas establecidas y procedimientos de la organización.

FOM_ORG.1 Responsabilidades de gestión

436 Dependencias: FOD_ORG.1 Responsabilidades de coordinación de seguridad

437 FOM_ORG.1.1 La OSF deberá definir [asignación: responsabilidades] para la gestión de forma que se asegure que las actividades de seguridad cumplen con la política de seguridad, se aprueban metodologías específicas y procesos para la seguridad de la información, se monitorizan cambios en las amenazas

significativas y en la exposición de los activos de información a amenazas, se evalúa la idoneidad y se coordina la implementación de controles de seguridad de la información específicos para sistemas o servicios nuevos, y se promueve la visibilidad de apoyo para la seguridad de la información en toda la organización.

438 FOM_ORG.1.2 La OSF deberá definir [asignación: responsabilidades] para los administradores de forma que se asegure que todos los procedimientos de seguridad dentro del área de su responsabilidad se llevan a cabo correctamente para cumplir con las políticas de seguridad y estándares.

439 FOM_ORG.1.3 La OSF deberá definir [asignación: responsabilidades] para la gestión de la revisión de la política de seguridad de la información de forma periódica o cuando ocurran cambios significativos, de forma que se garantice su conveniencia, idoneidad y eficacia.

FOD_ORG.1 Responsabilidades de coordinación de seguridad

440 Dependencias: no existen dependencias.

441 FOD_ORG.1.1 La OSF deberá definir [asignación: responsabilidades] de forma que las actividades de seguridad de la información estén coordinadas por representantes de diferentes partes de la organización con roles importantes y funciones de trabajo.

442 FOD_ORG.1.2 La OSF deberá definir [asignación: requisitos de seguridad] de forma que se mantengan contactos adecuados con autoridades importantes.

443 FOD_ORG.1.3 La OSF deberá definir [asignación: requisitos de seguridad] de forma que se mantengan contactos adecuados con grupos de especial interés u otros foros de seguridad especializados.

Gestión de sistemas TI

Gestión de actualizaciones

FOS_POL.1 Requisitos de seguridad

444 Dependencias: FOM_PRM.2 Segregación de privilegios.

445 FOS_POL.1.1 La OSF deberá definir [asignación: procedimientos] relativos a los procesos de gestión de la actualización de software para asegurar que se instalan los últimos parches aprobados y las actualizaciones de las aplicaciones para todo el software autorizado.

446 FOS_POL.1.2 La OSF deberá definir [asignación: procedimientos] relativos a la identificación de cambios en las instalaciones y sistemas de proceso de la información y su evaluación ante impactos potenciales.

447 FOS_POL.1.3 La OSF deberá definir [asignación: procedimientos] para el control de cambios formal, de forma que se controle la implementación de los cambios en los sistemas y las instalaciones que procesan información.

448 FOS_POL.1.4 La OSF deberá definir [asignación: procedimientos] para el mantenimiento y copia de librerías de programas de acuerdo con el control de cambios.

449 FOS_POL.1.5 La OSF deberá definir [asignación: procedimientos] de forma que los sistemas de información se comprueben regularmente para el cumplimiento de los estándares de implementación de seguridad.

450 FOS_POL.1.6 La OSF deberá especificar [asignación: controles de seguridad] en la declaración de los requisitos de negocio para los nuevos sistemas de información, o para la mejora de los sistemas de información existentes.

451 FOS_POL.1.7 La OSF deberá definir [asignación: procedimientos] para controlar la instalación de software en los sistemas operacionales.

452 FOS_POL.1.8 La OSF deberá definir [asignación: procedimientos] de forma que cuando los sistemas operativos sean cambiados, las aplicaciones críticas para el negocio se revisen y se comprueben para asegurarse que no hay un impacto negativo en las operaciones o en la seguridad de la empresa.

453 FOS_POL.1.9 La OSF deberá definir [asignación: reglas] que contemplen que no se recomiendan las modificaciones de los paquetes software, y que éstas se limitan exclusivamente a los cambios necesarios, estando además todos los cambios estrictamente controlados.

454 FOS_POL.1.10 La OSF deberá documentar, mantener y tener disponible [asignación: procedimientos] para todos los usuarios que los necesiten.

455 **Nota de aplicación:**

- Con el objeto de evitar la existencia de vulnerabilidades explotables en productos COTS que formen parte del STOE y que se publican en el dominio público, es necesaria la existencia de la función del personal administrador del dominio soporte para la realización de instalaciones de los COTS con políticas de seguridad, de mantenimiento al día de parches y hotfixes de sistemas operativos y demás productos COTS utilizados.

- Esta función incluirá la configuración y revisión de las reglas del firewall y la monitorización de los sistemas de detección de intrusos, monitorización del tráfico y uso de la red.

FOM_PRM.2 Segregación de privilegios

456 Dependencias: no existen dependencias.

457 FOM_PRM.2.1 La OSF deberá definir [asignación: reglas] que contemplen la segregación de privilegios para reducir la posibilidad de una modificación no autorizada o el mal uso de los activos, de forma que se lleve a cabo la separación de la inicialización de un evento de su autorización.

458 FOM_PRM.2.2 La OSF deberá definir [asignación: requisitos de seguridad] en la asignación de privilegios a identidades de usuario diferentes de aquellas que se utilizan normalmente para el negocio.

459 **Nota de aplicación:**

- Para el dominio OPERADORES INTERNOS, se debe definir la política de control de acceso a los activos y demás información crítica de seguridad asociada a las aplicaciones de formalización de las apuestas, basada en los roles de operario y administrador.
- Así mismo, en el dominio SOPORTE se deberá definir una política de control de acceso a los componentes que dan soporte a la seguridad global del STOE y a las aplicaciones. Dicha política estará basada en los roles (administrador, usuario) especificados para el dominio. Ejemplos de componentes incluidos en este dominio serían los sistemas operativos, los sistemas de gestión de base datos, firewall, IDS, etc.

Política anti-malware

FOS_POL.2 Política de código malicioso

460 Dependencias: no existen dependencias.

461 FOS_POL.2.1 La OSF deberá definir [asignación: procedimientos] para la gestión del tratamiento de la protección contra código malicioso en los sistemas, informando y recuperándose de los ataques de código malicioso.

462 FOS_POL.2.2 La OSF deberá definir [asignación: procedimientos] para la detección y la protección contra código malicioso que se pudiera ser transmitido a través del uso de la red de comunicaciones.

463 FOS_POL.2.3 La OSF deberá definir [asignación: responsabilidades] para tratar la protección contra el código malicioso en los sistemas, ejercitándose en su uso, informando y recuperándose de ataques de código malicioso.

464 FOS_POL.2.4 La OSF deberá definir [asignación: procedimientos] para implementar controles para la detección, prevención y recuperación de la protección contra código malicioso, además de una concienciación adecuada de los usuarios.

465 **Nota de aplicación:**

- Será necesario la instalación y mantenimiento al día de un antivirus. La configuración de los servidores no deberá permitir a los usuarios del dominio OPERADORES INTERNOS la desactivación del antivirus (como parte de la política de control de acceso del dominio SOPORTE).

- Existirán antivirus en: las estaciones de trabajo (los PCs), los servidores de ficheros, servidores de aplicaciones, servidores de base de datos, servidores de correo, tráfico HTTP y FTP (bien en gateway o en el firewall).

Copias de seguridad

FOS_OAS.2 Procedimientos de copias de respaldo

466 Dependencias: no existen dependencias.

467 FOS_OAS.2.1 La SSF deberá proporcionar [asignación: procedimientos] para llevar a cabo y probar copias de respaldo de la información y el software de forma regular de acuerdo con la política de copias de respaldo acordada.

468 FOS_OAS.2.2 La OSF deberá definir [asignación: procedimientos] para generar un nivel adecuado de copias de respaldo, junto con un registro preciso y completo de las copias de respaldo, además de procedimientos de restauración documentados.

469 FOS_OAS.2.3 La OSF deberá definir [asignación: procedimientos] para dispositivos de almacenamiento de copias de respaldo de forma que se pueda asegurar que pueden ser utilizados en caso de emergencia.

470 FOS_OAS.2.4 La OSF deberá definir [asignación: procedimientos] para asegurar que son efectivos y que se se pueden llevar a cabo dentro del tiempo establecido en los procedimientos operacionales para la recuperación.

471 FOS_OAS.2.5 La OSF deberá definir [asignación: requisitos de seguridad] en la gestión de copias de respaldo para los sistemas individuales de forma que se pueda asegurar que cumplen los requisitos del plan de continuidad de negocio.

472 **Nota de aplicación:**

- El documento de política de seguridad deberá incluir procedimientos para la realización de copias de seguridad. El fabricante deberá definir e implantar los mecanismos técnicos (herramientas) para la realización de las copias conforme a los procedimientos. Los procedimientos incluirán el chequeo regular (como mínimo cada tres meses) de la validez de las copias: posibilidad de restaurar el sistema con las copias existentes (FOS_OAS.2.1).

- Se deberá definir un responsable de la gestión las copias de seguridad: realización, etiquetado, almacenamiento seguro, inventario de los soportes de las copias, chequeo de las copias.

- Se almacenarán copias de respaldo actualizadas semanalmente (como mínimo) en una ubicación distinta a la ubicación en la que se realiza la actividad.

Registro y notificación de incidencias de seguridad

FOS_RCD.1 Registros

473 Dependencias: no existen dependencias.

474 FOS_RCD.1.1 La SSF deberá proporcionar [asignación: medidas] para registrar todos los fallos, sospechosos o reales, y para el mantenimiento mediante acciones correctivas de los equipos.

FOM_INC.1 Informe de los problemas de seguridad detectados

475 Dependencias: no existen dependencias.

476 FOM_INC.1.1 La OSF deberá definir [asignación: procedimientos] para anotar e informar de cualquier debilidad de seguridad observada o sospechosa, o de amenazas a sistemas o servicios, comunicándolo al administrador correspondiente o directamente al proveedor del servicio tan rápidamente como sea posible de forma que se eviten incidentes de seguridad.

477 FOM_INC.1.2 La OSF deberá definir [asignación: reglas] para prohibir el intento de que se pruebe la existencia de una debilidad sospechosa a través de múltiples intentos.

478 **Nota de aplicación:**

- El documento de política de seguridad deberá incluir un procedimiento de notificación, gestión y respuesta ante las incidencias que incluya la existencia de un registro de incidencias especificando tipo de incidencia, notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

- Además deberán consignarse, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Plan de continuidad del servicio

FOB_BCN.1 Análisis de impacto

479 Dependencias: FOD_RSM.1 Gestión de riesgos de la organización

480 FOB_BCN.1.1 La OSF deberá definir [

- Identificación de los eventos que puedan causar interrupciones al servicio, probabilidad, impacto y consecuencias para la seguridad de la información;
- Ante la ocurrencia de cualquier evento que ponga en peligro la continuidad del servicio, se garantizará que el personal necesario para garantizar la continuidad estará presente en las instalaciones no más tarde de los 25 minutos posteriores a la ocurrencia del evento.
- asignación: otros requisitos de seguridad]

llevando a cabo un análisis de impacto de negocio para identificar los eventos que podrían causar interrupciones de los procesos de negocio, además del cálculo de la probabilidad y el impacto de dichas interrupciones y de sus consecuencias para la seguridad de la información.

481 FOB_BCN.1.2 La OSF deberá definir [asignación: requisitos de seguridad] llevando a cabo análisis de impacto de la continuidad del negocio, involucrando a los propietarios de los recursos y de los procesos de negocio.

482 FOB_BCN.1.3 La OSF deberá definir [asignación: requisitos de seguridad] en los planes de continuidad de negocio para la recuperación de ataques de código malicioso, incluyendo todos los datos necesarios y las copias del respaldo de software, además de los procesos de recuperación.

483 FOB_BCN.1.4 La OSF deberá especificar [asignación: requisitos de seguridad] para la comprensión de los riesgos a los que se enfrenta la organización en términos de la probabilidad de impacto, comprensión del impacto que la interrupción probablemente tendrá en el negocio, formulando y documentando una estrategia de continuidad del negocio consistente con los objetivos y prioridades del negocio, formulando y documentando planes de continuidad de negocio en línea con la estrategia acordada, probando y actualizando los planes regularmente y los procesos puestos en marcha y asegurando que la gestión de la continuidad del negocio se incorpora a los procesos de la organización y estructura de la continuidad del negocio.

484 FOB_BCN.1.5 La OSF deberá definir [asignación: requisitos de seguridad] para el desarrollo e implementación de los planes de continuidad de negocio para mantener y restaurar las operaciones y para asegurar la disponibilidad de la información al nivel requerido y según el tiempo establecido después de que se produzca la interrupción, o fallo, de los procesos de negocio críticos.

485 FOB_BCN.1.6 La OSF deberá definir [asignación: procedimientos] para el almacenamiento en un lugar remoto de copias de los planes de continuidad de negocio, a una distancia adecuada para que no sufran ningún daño proveniente del desastre producido en el sitio principal. Deberá asegurarse que esas copias están actualizadas y protegidas al mismo nivel de seguridad que la del sitio principal.

486 FOB_BCN.1.7 La OSF deberá especificar [asignación: requisitos de seguridad] para las condiciones de su activación, así como a los responsables de ejecutar cada componente del plan para cada plan de continuidad de negocio.

487 FOB_BCN.1.8 La OSF deberá definir [asignación: requisitos de seguridad] para la prueba y actualización de los planes de continuidad de negocio para asegurar que están al día y son efectivos.

488 FOB_BCN.1.9 La OSF deberá definir [asignación: requisitos de seguridad] en los planes de aislamiento de fallos de forma que el impacto de un fallo tenga un mínimo impacto en la continuidad del negocio cuando ocurra un incidente de seguridad.

489 FOB_BCN.1.10 La OSF deberá definir [asignación: reglas] para la definición de un acceso especial a los recursos del sistema operacional en el momento en el que se produzcan los fallos de seguridad.

490 FOB_BCN.1.11 La OSF deberá definir [asignación: requisitos de seguridad] de forma que se desarrolle y mantenga un proceso gestionado para la continuidad del negocio en toda la organización que contemple los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

491 FOB_BCN.1.12 La OSF deberá definir [asignación: requisitos de seguridad] para un marco conjunto de planes de continuidad de negocio para asegurar que todos los planes son consistentes, tratan de forma consistente los requisitos de seguridad de la información, e identifican las prioridades para las pruebas y el mantenimiento.

Instalaciones y equipamiento

FOP_RMM.1 Gestión de los Dispositivos Removibles

492 Dependencias: no existen dependencias.

493 FOP_RMM.1.1 La OSF deberá definir [asignación: procedimientos] para la gestión de dispositivos removibles.

494 FOP_RMM.1.2 La OSF deberá definir [asignación: procedimientos] para la autorización del traslado de dispositivos removibles de la organización.

495 FOP_RMM.1.3 La OSF deberá definir [asignación: procedimientos] para la minimización de riesgos relativos con el filtrado de información sensible a personas no autorizadas, estableciendo procedimientos formales para la destrucción segura de dispositivos.

496 FOP_RMM.1.4 La OSF deberá definir [asignación: procedimientos] para el borrado de contenidos, que incluya cualquier dato sensible y software autorizado, de cualquier dispositivo y equipo que contenga , de forma que se

eliminen de la organización cuando no hagan falta y se compruebe que realmente que así ha sido.

497 **Nota de aplicación:**

- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

- Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

- Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario (FDP_RIP.1 Subconjunto de la protección de la información residual / BACKUPS).

- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos (FCS_COP.1 Operación criptográfica / CIFRADO DE BACKUPS).

FOP_SYS.1 Gestión del Equipo del Sistema

498 Dependencias: no existen dependencias.

499 FOP_SYS.1.1 La OSF deberá definir [asignación: reglas] para equipos de emergencia en el sitio y para que los dispositivos con las copias de respaldo estén a una distancia segura para evitar el daño de un posible desastre en el sitio principal.

500 FOP_SYS.1.2 La OSF deberá definir [asignación: reglas] para guardar los materiales peligrosos y el combustible a una distancia segura de un área segura.

501 FOP_SYS.1.3 La OSF deberá definir [asignación: reglas] para guardar listados y directorios de teléfonos internos que identifiquen sitios donde se procesa información sensible no accesible al público.

502 FOP_SYS.1.4 La OSF deberá definir [asignación: procedimientos] para inspeccionar el material entrante de amenazas potenciales antes de que se mueva del área de entrega y carga, al punto de utilización.

503 FOP_SYS.1.5 La SSF deberá proporcionar [asignación: medidas] para la protección del cableado de red de intercepciones no autorizadas o del peligro proveniente de las zonas públicas.

504 FOP_SYS.1.6 La OSF deberá definir [asignación: reglas] para mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor.

505 FOP_SYS.1.7 La OSF deberá definir [asignación: reglas] de forma que sólo el personal de mantenimiento autorizado debería llevar a cabo la reparación y servicio del equipo.

506 FOP_SYS.1.8 La OSF deberá definir [asignación: controles] para un nivel apropiado de protección física y de entorno consistente con los estándares aplicados en el sitio principal para las copias de respaldo. Los controles aplicados a los dispositivos en el sitio principal deberán extenderse al sitio de respaldo.

507 FOP_SYS.1.9 La OSF deberá definir [asignación: reglas] para guardar todos los dispositivos en una caja fuerte y en un entorno seguro de acuerdo a la especificación del fabricante.

508 FOP_SYS.1.10 La OSF deberá definir [asignación: responsabilidades] para proteger cada equipo no atendido por todos los empleados, contratistas y terceras partes, según los requisitos y procedimientos de seguridad.

509 FOP_SYS.1.11 La OSF deberá definir [asignación: procedimientos] para asegurar que toda la información relevante se transfiere a la organización y se borra de forma segura de los equipos, en caso de que el empleado, contratista y terceras partes compren equipos de la organización o usen sus equipos personales.

510 FOP_SYS.1.12 La OSF deberá proporcionar [asignación: controles] para los dispositivos que contengan información que deba ser protegida de acceso no autorizado, mal uso o daño durante el transporte más allá de los límites físicos de la organización.

511 **Nota de aplicación:**

- Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan.

- Respecto a la seguridad del cableado:

  - Las líneas de energía y telecomunicaciones en las zonas de tratamiento de información, se enterrarán, cuando sea posible, o se adoptarán medidas alternativas de protección.

  - La red cableada se protegerá contra intercepciones no autorizadas o daños, por ejemplo, usando conductos y evitando rutas a través de áreas públicas.

  - Se segregarán los cables de energía de los de comunicaciones para evitar interferencias.

  - Se considerarán medidas adicionales para sistemas sensibles o críticos, como:

    - instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación;
    - uso de rutas o de medios de transmisión alternativos;
    - uso de cableado de fibra óptica;
    - inicialización de barreras contra el enganche a los cables de dispositivos no autorizados.

FOP_MNG.1 Seguridad física

512 Dependencias: FOD_PSN.5 Acceso a instalaciones y equipos

513 FOP_MNG.1.1 La OSF deberá definir [asignación: requisitos de seguridad] de seguridad física de las oficinas, habitaciones e instalaciones contra los daños de fuego, inundaciones, terremotos, explosiones, disturbios y otras formas de daños naturales o causados por el hombre.

514 FOP_MNG.1.2 La OSF deberá definir [asignación: requisitos de seguridad] para la separación de las instalaciones de desarrollo, de pruebas y de operación, para reducir el riesgo de acceso no autorizado o de cambios en el sistema operacional.

515 FOP_MNG.1.3 La OSF deberá definir [asignación: requisitos de seguridad] para proporcionar instalaciones donde se encuentren las copias de respaldo, de forma que sea pueda recuperar la información esencial y el software después de un desastre o fallo en los dispositivos.

516 FOP_MNG.1.4 La OSF deberá definir [asignación: requisitos de seguridad] para la protección de las instalaciones de proceso de información, para evitar el acceso no autorizado o revelación de información almacenada y procesada en estas instalaciones.

517 **Nota de aplicación:**

– Se deberán considerar los siguientes aspectos cuando sean de aplicación:

- **Áreas seguras**
  - **Perímetro de seguridad física**

518 La protección física se logra creando una serie de barreras físicas en torno a los locales de la Organización y a los recursos de tratamiento de la información. Cada barrera establece un perímetro de seguridad que aumenta la protección total:

519 El perímetro de seguridad estará claramente definido.

520 El perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debe tener solidez física (por ejemplo no tendrá zonas que puedan derribarse fácilmente).

521 Se instalará un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se restringirá sólo al personal autorizado.

522 Las barreras físicas se extenderán si es necesario desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno (como la causada por incendios o inundaciones).

523 Todas las puertas para incendios del perímetro de seguridad tendrán alarma y cierre automático.

  - **Controles físicos de entradas**

524 Las áreas de seguridad estarán protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado. Deben considerarse los siguientes aspectos:

525 Las visitas a estas áreas se supervisarán u ordenarán y se registrarán su fecha y momentos de entrada y salida. Los visitantes sólo tendrán acceso para propósitos especificados y autorizados, proporcionándoles instrucciones sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

526 Se controlará y restringirá sólo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento.

527 Se exigirá a todo el personal que lleve alguna forma de identificación visible.

528 Se revisarán y actualizarán regularmente los derechos de acceso a áreas de seguridad.

○ Seguridad de oficinas, despachos y recursos

529 Los recursos críticos se situarán fuera de áreas de acceso público.

530 Los edificios deberán ser discretos y dar mínimas indicaciones de su propósito, sin signos obvios (fuera o dentro del edificio) que identifiquen la presencia de actividades informáticas.

531 Las funciones y equipos de soporte (por ejemplo fotocopiadoras, faxes, etc.) se situarán en el área de seguridad adecuadamente para evitar demandas de acceso que puedan debilitar la seguridad de la información.

532 Las ventanas y puertas permanecerán cerradas cuando la instalación esté vacía. Se tendrá protección externa en las ventanas, sobre todo en las de planta baja.

533 Se instalarán sistemas de detección de intrusos normalizados profesionalmente y se probarán regularmente para cubrir todas las puertas externas y las ventanas accesibles. Las alarmas de espacios no ocupados estarán activadas permanentemente. También se cubrirán otras áreas como las salas de tratamiento de datos y comunicaciones.

534 Los recursos de tratamiento de información utilizados por la Organización se separarán físicamente de los usados por terceros.

535 El público no accederá automáticamente a los directorios de los vestíbulos y de los teléfonos internos de la Organización que identifiquen lugares con recursos de tratamiento de información sensible.

536 Los materiales peligrosos y combustibles se almacenarán de forma segura a una distancia de seguridad de un área segura. No se almacenarán dentro de un área de seguridad suministros a granel -como material de escritorio- hasta que se necesiten.

537 El equipamiento y los soportes de respaldo estarán a una conveniente distancia de seguridad para evitar que se dañen por un desastre en el área principal.

○ El trabajo en las áreas de seguridad

538 Pueden requerirse controles y normas adicionales para asegurar más un área de seguridad:

539 El personal sólo conocerá la existencia de un área de seguridad, o de sus actividades, si lo necesitara para su trabajo.

540 Se evitará el trabajo no supervisado en áreas de seguridad tanto por motivos de salud como para evitar oportunidades de actividades maliciosas.

541 Las áreas seguras estarán cerradas y se controlarán periódicamente cuando estén vacías.

542 El personal de servicios de soporte de terceros, debidamente autorizado, sólo accederá a las áreas de seguridad o a recursos de tratamiento de información sensible cuando sea requerido y su acceso se monitorizará.

543 No se permitirá la presencia de equipos de fotografía, video, audio u otras formas de registro salvo autorización especial.

- **Áreas aisladas de carga y descarga**

544 Se controlarán áreas de carga y descarga - y se aislarán en lo posible- separadas de los recursos de tratamiento de información para evitar accesos no autorizados:

545 Se restringirán los accesos al área de carga y descarga desde el exterior sólo para el personal autorizado e identificado.

546 El área se diseñará para que los suministros puedan descargarse sin tener acceso a otras zonas del edificio.

547 La puerta externa del área debe estar cerrada cuando la interna esté abierta.

548 El material entrante se inspeccionará para evitar amenazas potenciales antes de llevarlo a su lugar de utilización.

549 El material entrante se registrará si cabe al entrar en el lugar.

- **Seguridad de los equipos**
  - **Instalación y protección del Equipamiento**

550 El equipamiento debe situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. Los siguientes controles deben ser considerados:

551 Los equipos se situarán donde se minimicen los accesos innecesarios a las áreas de trabajo.

552 Los equipos de tratamiento y almacenamiento de información que manejen datos sensibles se instalarán donde se reduzca el riesgo de que otros vean los procesos durante su uso.

553 Los elementos que requieran especial protección se aislarán para reducir el nivel general de protección requerido.

554 Se adoptarán medidas para minimizar los riesgos de amenazas potenciales como las siguientes:

- Robo
- Incendio
- Explosivos
- Humo
- Agua (o fallo de suministro)
- Polvo
- Vibraciones
- Agentes químicos
- Interferencias en el suministro eléctrico
- Radiaciones electromagnéticas

555 La política de la Organización prohibirá fumar, beber y comer cerca de los equipos de tratamiento de información.

556 Se vigilarán las condiciones ambientales que puedan afectar negativamente la operación de los equipos de tratamiento de información.

557 Para los equipos situados en ambientes industriales se considerará el uso de métodos de protección especial (por ejemplo cubiertas para teclados).

558 Se considerarán los impactos de desastres que puedan ocurrir en lugares próximos, tanto vertical como horizontalmente (por ejemplo el incendio en el edificio vecino, fugas de agua en pisos superiores o una explosión en la calle).

FOP_MNG.2 Utilidades de apoyo en caso de fallo de corriente

559 Dependencias: no existen dependencias.

560 FOP_MNG.2.1 La SSF deberá proporcionar [asignación: controles] utilidades de apoyo para la protección de los equipos ante fallos de corriente y otras interrupciones causadas por fallos.

561 FOP_MNG.2.2 La OSF deberá definir [asignación: requisitos de seguridad] para el uso de equipos de SAI (Sistema de Alimentación Ininterrumpida).

562 FOP_MNG.2.3 La OSF deberá definir [asignación: requisitos de seguridad] para el uso de un generador de copias de respaldo si el procesamiento tiene que ser continuo en caso de que se produzca un fallo de corriente prolongado.

563 **Nota de aplicación:**

- Se deberán considerar los siguientes aspectos cuando sean de aplicación:
    - Se cubrirá mediante planes de contingencia las acciones a adoptar en caso de fallos de suministro y necesidad de uso del SAI y en caso de fallo del SAI.
    - Los equipos SAI se revisarán regularmente para asegurar que tienen la capacidad adecuada y que están probados de acuerdo con las recomendaciones del fabricante.

Requisitos de garantía de seguridad

564 Los requisitos de garantía que se especifican en esta sección son comunes para los tres dominios declarados en la sección Organización de dominios.

565 La evaluación global del sistema especifica actividades asociadas a la evaluación de la declaración de seguridad del sistema (SST) y actividades asociadas a la evaluación del STOE.

Requisitos de garantía asociados a la evaluación de SST

566 Se establecen los siguientes requisitos de garantía para la evaluación de la declaración de seguridad del sistema (SST) según se especifican en [ISO19791]:

- SST Introducción (ASS_INT)

ASS_INT.1 SPP Introducción

- Declaración de conformidad (ASS_CCL)

  ASS_CCL.1 Declaración de conformidad

- Definición del problema de seguridad (ASS_SPD)

  ASS_SPD.1 Definición del problema de seguridad

- Objetivos de seguridad (ASS_OBJ)

  ASS_OBJ.1 Objetivos de seguridad

- Definición de componentes extendidos (ASS_ECD)

  ASS_ECD.1 Definición de componentes extendidos

- Requisitos de seguridad (ASS_REQ)

  ASS_REQ.2 Requisitos de seguridad derivados

- Especificación resumida del STOE (ASS_TSS)

  ASS_TSS.1 Especificación resumida del STOE

- Introducción del dominio de seguridad (ASS_DMI)

  ASS_DMI.1 Introducción del dominio de seguridad

- Declaración de conformidad del dominio de seguridad (ASS_DMC)

  ASS_DMC.1 Declaración de conformidad del dominio de seguridad

- Definición del problema de seguridad del dominio de seguridad (ASS_DMP)

  ASS_DMP.1 Definición del problema de seguridad del dominio de seguridad

- Objetivos de seguridad del dominio de seguridad (ASS_DMO)

  ASS_DMO.1 Objetivos de seguridad del dominio de seguridad

- Requisitos de seguridad del dominio de seguridad (ASS_DMR)

  ASS_DMR.2 Requisitos de seguridad del dominio de seguridad derivados

- Especificación resumida del dominio de seguridad (ASS_DMS)

  ASS_DMS.1 Especificación resumida del dominio de seguridad

Requisitos de garantía asociados a la evaluación de STOE

567 Los requisitos de garantía correspondientes a la evaluación del STOE, se establecen para cubrir todas las fases del ciclo de vida del sistema:

- Desarrollo / Integración
- Instalación
- Operación
- Modificación

568 En las siguientes secciones se establecen los requisitos de garantía para la evaluación del STOE por fases del ciclo de vida según se especifican en [ISO19791].

569 El detalle de cada una y metodología de evaluación se especifica en [ISO19791].

Desarrollo/ Fase de integración

Clase	Familia / Componente	
AOD Manuales	AOD_OCD.1	Descripción de la especificación de la configuración
	AOD_OGD.1	Descripción del usuario relativo a las SSFs en el manual de usuario
ASD Diseño	ASD_SAD.1	Descripción de la arquitectura
	ASD_CON.1	Concepto de seguridad de operación
	ASD_IFS.1	Descripción de los interfaces externos
	ASD_STD.1	Descripción del diseño del STOE: diseño de subsistemas
AOT Pruebas	AOT_COV.1	Pruebas de cobertura para las SFFs: evidencia de cobertura
	AOT_DPT.1	Pruebas de profundidad para el diseño de subsistemas
	AOT_FUN.1	Pruebas funcionales de las SSFs

Fase de Instalación

Clase	Familia / Componente	
AOD Manuales	AOD_OCD.2	Verificación de la especificación de la configuración
AOC Gestión de la Configuración	AOC_OBM.1	Gestión de la Configuración de Operación: Configuración del sistema operacional
	AOC_ECP.1	Configuración de los componentes evaluados: Componentes evaluados
	AOC_UCP.1	Configuración de los componentes no evaluados: Componentes no evaluados
AOT Pruebas	AOT_COV.1	Pruebas de cobertura de las SFFs: Evidencia de cobertura
	AOT_DPT.1	Pruebas de profundidad para el diseño de

		subsistemas
	AOT_FUN.1	Pruebas funcionales de las SSFs
	AOT_IND.1	Pruebas independientes - conformidad
AOV Análisis de Vulnerabilidades	AOV_VAN.6	Evaluación de las vulnerabilidades: Análisis de vulnerabilidades metódico
APR Preparación para la operación real	APR_AWA.1	Formación de concienciación
	APR_CMM.1	Comunicación en las SSFs al personal apropiado
	APR_SIC.1	Instalación segura y puesta en marcha del STOE

Fase de Operación

Clase	**Familia / Componente**	
AOD Manuales	AOD_OGD.2	Verificación del uso de las SSFs en el manual de usuario
APR Preparación de la operación real	APR_AWA.2	Verificación de la formación de concienciación
	APR_CMM.2	Verificación de la comunicación en las SSFs a el personal
	APR_SIC.2	Verificación de la instalación segura y puesta en marcha
ASO Registros en el Sistema Operacional	ASO_RCD.1	Verificación de los registros operacionales: Registro de los controles operacionales
	ASO_VER.1	Verificación de los controles operacionales
	ASO_MON.1	Gestión de la monitorización de las SSFs: Monitorización de los controles operacionales a través de la gestión

Fase de Modificación

Clase	Familia / Componente	
AOD Manuales	AOD_GVR.1	Verificación de los manuales
ASD Diseño	ASD_RVR.1	Verificación de requisitos
	ASD_DVR.1	Verificación del diseño
AOT Pruebas	AOT_REG.1	Pruebas de regresión
AOV Análisis de Vulnerabilidades	AOV_VAN.6	Pruebas de penetración Evaluación de las vulnerabilidades: Análisis de vulnerabilidades metódico

Justificación de los requisitos de seguridad

Cumplimiento del Reglamento de Apuestas de la Ciudad de Ceuta

570 Se incluye, a continuación, la justificación de cumplimiento de los requisitos de seguridad de los sistemas en el caso de formalización de apuestas por medios informáticos o electrónicos interactivos, según el artículado de [RACC].

571 En la justificación se incluye el identificador de requisito técnico u operacional que se ha especificado en la sección de requisitos de seguridad para cada dominio.

Artículo [RACC]	Requisito [RACC]	Artículo/ Requisito en el PPS de la instrucción
Artículo 8	1. k) Certificación de una empresa auditora, con personal acreditado en auditorías de seguridad informática, sobre la solvencia técnica del sistema informático previsto para la organización y comercialización de las apuestas.	Artículo 2: Certificación del sistema conforme al PPS por parte del CCN
Artículo 10, 18	a) Validar las apuestas realizadas por los usuarios …….	Desde el punto de vista de la seguridad, el proceso de validación de las apuestas de los usuarios implica la verificación de la firma de la apuesta que garantiza la identidad del apostante y el no repudio y el chequeo de integridad de la misma. Para ellos se debenrán implementar los siguientes requisitos: Dominio OPERADORES INTERNOS: requisitos de verificación de la firma electrónica del cliente en su apuesta: FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS, FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS

Artículo 20	1. Los sistemas, elementos o instrumentos técnicos utilizados para la organización y comercialización de las apuestas garantizarán su autenticidad y cómputo, la identidad de las personas intervinientes, en su caso, la confidencialidad y seguridad respecto de los datos de carácter personal recabados, ……	Respecto a los tres dominios: • Requisitos de I&A (FIA_UID.2, FIA_UAU.2) • Requisitos que implementan las políticas de control de acceso (FDP_ACC.2, FDP_ACF.1). Dominio CLIENTES: • Requisitos de garantía de comunicaciones con las pasarelas de pago FTP_ITC.1 Canal seguro Inter-TSF / PASARELA DE PAGO • Requisitos de Auditoría. FAU_GEN.1 Generación de datos de auditoría / CLIENTES FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES Dominio OPERADORES INTERNOS: • Requisitos de generación de la firma de las apuestas de los clientes: FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS • Requisitos de verificación de las apuestas de los clientes mediante mecanismos de firma electrónica FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS, FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS. • Garantía integridad en las apuestas y boletos almacenados.

		FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO • Garantía de no repudio por parte de la entidad y del cliente. FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS, FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS. FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO • Establecimiento de requisitos de aleatoriedad si fuera precisa en algún tipo de apuesta. FCS_RNG.1 Generación de números aleatorios • Comunicaciones seguras con los clientes, consejería y otros mercados. FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES • Requisitos de Auditoría. FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES Dominio SOPORTE: • Requisitos de redundancia y tolerancia a fallos. FRU_FLT.2 Tolerancia a fallos limitada, FPT_RCV.2 Recuperación automática • Mecanismos criptográficos para cifrar los discos en los que se almacenan las apuestas, boletos y datos de carácter personal sujetos a [LOPD]. FCS_COP.1 Operación criptográfica / CIFRADO DE DISCOS

		FCS_COP.1 Operación criptográfica / CIFRADO DE BACKUPS • Realización de copias de respaldo y cifrado de las mismas: recuperación del sistema y mantenimiento de la confidencialidad de los datos de carácter personal, apuestas, etc. FOP_RMM.1 Gestión de los Dispositivos Removibles FOS_OAS.2 Procedimientos de copias de respaldo • Borrado de los soportes con copias de seguridad que contengan datos de carácter personal o cuando éstos vayan a ser destruido o reutilizados: FDP_RIP.1 Protección de un subconjunto de la información residual / BACKUPS • Establecmiento de una fuente fiable de tiempos para sellar las apuestas. FPT_STM.1 Sellados de tiempo fiables • Requisitos de Auditoría para detección de intrusos. FAU_GEN.1 Generación de datos de auditoría / SOPORTE FAU_STG.1 Protección de la traza de auditoría almacenada / SOPORTE FOS_RCD.1 Registros FOM_INC.1 Informe de los problemas de seguridad detectados FOS_MON.1 Registros de auditoría • Requisitos de seguridad físicos del local. FOP_SYS.1 Gestión del Equipo del Sistema FOP_MNG.1 Seguridad física FOP_MNG.2 Utilidades de apoyo en caso de fallo de corriente • Establecimiento de procedimientos de gestión de la seguridad: establecimiento de una política de seguridad, gestión de personal, instalaciones, copias de respaldo, gestión de los ficheros con datos de carácter personal, etc. (A)

		FOD_PSN.1 Roles y responsabilidades del personal FOD_POL.1 Security policy (B) FOM_PSN.2 Security managers FOM_ORG.1 Management responsibilities FOD_ORG.1 Security coordination responsibilities (C) FOP_RMM.1 Gestión de los Dispositivos Removibles FOS_OAS.2 Procedimientos de copias de respaldo (D) [LOPD] FOD_POL.2 Protección de datos y política de privacidad FOA_PRO.1 Privacidad de los datos FOM_CLS.2 Identificación de Activos FOM_PSN.1 Propiedad de los activos FOA_INF.1 Data protection
	3. El sistema técnico deberá permitir, al menos, el análisis de los riesgos y la continuidad del negocio, así como la determinación y subsanación de sus vulnerabilidades	Dominio SOPORTE: • Desarrollo y mantenimiento de la política de seguridad. (A) FOD_PSN.1 Roles y responsabilidades del personal FOD_POL.1 Security policy FOD_RSM.1 Risk management within the organization (B) FOM_PSN.2 Security managers FOM_ORG.1 Management responsibilities FOD_ORG.1 Security coordination responsibilities • Requisitos de Auditoría para detección de

		intrusos. FAU_GEN.1 Generación de datos de auditoría / SOPORTE FAU_STG.1 Protección de la traza de auditoría almacenada / SOPORTE FAU_SAA.1 Análisis de violaciones potenciales FOS_RCD.1 Registros FOM_INC.1 Informe de los problemas de seguridad detectados FOS_MON.1 Registros de auditoría FPT_STM.1 Sellados de tiempo fiables • Mantenimiento del equipamiento en ámbito de la seguridad. FOS_POL.2 Malicious code policy FOS_POL.1 Security requirements (updates) • Desarrollo del Plan de continuidad del negocio ("BCP"). FOB_BCN.1 Impact analysis
	a) Mecanismos que permitan seguir o rastrear el registro de las operaciones de apuestas realizadas, garantizando su integridad y su asociación temporal a fuentes de tiempo fiables.	Dominio SOPORTE: • Fuente fiable de tiempo FPT_STM.1 Sellados de tiempo fiables Dominio OPERADORES INTERNOS: • Requisitos de generación de la firma de las apuestas de los clientes: FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS Se verifica la firma de las apuestas (la del cliente – FCS_COP.1 Operación criptográfica /

		VERIFICAR HASH CLIENTE APUESTAS) y se almacenan los datos garantizando su intergidad (FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS). Se genera el boleto asociado que se envía firmado por la entidad al cliente (FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO). En ese momento se considera formalizada y aceptada la apuesta. Este proceso garantiza el no repudio en ambos lados y la integridad de los datos de las apuestas y boleto almacenados, por lo que se garantiza su trazabilidad, asignándole una medida fiable de tiempo (FPT_STM.1 Reliable time stamps). • Los requisitos de redundancia (FRU_FLT.2 Tolerancia a fallos limitada , y recuperación (FPT_RCV.2 Recuperación automática) y copias de resplado garantizan la reconstrucción del sistema y su disponiblidad (FOP_RMM.1 Gestión de los Dispositivos Removibles FOS_OAS.2 Back-up procedures) • Requisitos de Auditoría en CLIENTES y OPERADORES con protección de la traza obtenida. FAU_GEN.1 Generación de datos de auditoría / CLIENTES FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES

	b) Mecanismos de autenticación íntimamente ligados a la explotación del sistema informático, de dispositivos físicos que garanticen el control de acceso a los componentes del sistema informático solo a personal autorizado.	(A) Seguridad lógica Respecto a los tres dominios: Requisitos de I&A (FIA_UID.2, FIA_UAU.2) Requisitos que implementan las políticas de control de acceso (FDP_ACC.2, FDP_ACF.1). (B) Seguridad física FOP_MNG.1 Seguridad física
	c) Mecanismos que aseguren la confidencialidad e integridad en las comunicaciones con el apostante y entre los componentes del sistema informático.	Requisitos de comunicaciones seguras: Dominio CLIENTES: • Requisitos de garantía de comunicaciones con las pasarelas de pago FTP_ITC.1 Canal seguro Inter-TSF / PASARELA DE PAGO Dominio OPERADORES INTERNOS: • Comunicaciones seguras con los clientes, consejería y otros mercados. FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES
Artículo 21	2. La configuración de la Unidad Central de Apuestas permitirá que se pueda comprobar en cualquier momento las operaciones de apuestas y sus resultados, así como reconstruir de forma fiel las transacciones realizadas, impidiendo cualquier modificación o alteración de las operaciones realizadas	Dominio CLIENTES: • Auditoría FAU_GEN.1 Generación de datos de auditoría / CLIENTES FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES FPT_STM.1 Sellados de tiempo fiables Dominio OPERADORES INTERNOS: • Auditoría FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES

		FPT_STM.1 Sellados de tiempo fiables • Traza FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO Dominio SOPORTE: • Auditoría: FAU_GEN.1 Generación de datos de auditoría / SOPORTE FAU_STG.1 Protección de la traza de auditoría almacenada / SOPORTE FOS_RCD.1 Registros FOS_MON.1 Registros de auditoría FPT_STM.1 Sellados de tiempo fiables • Redundancia y restauración: FRU_FLT.2 Tolerancia a fallos limitada , FPT_RCV.2 Recuperación automática FOP_RMM.1 Gestión de los Dispositivos Removibles FOS_OAS.2 Procedimientos de copias de respaldo
	3. El acceso a la Unidad Central de Apuestas requerirá la adopción de medidas de control que permitan registrar todas las actuaciones u operaciones realizadas en ella y utilizar mecanismos de autenticación de los operarios.	Para todos los dominios: - Identificación y Autenticación (FIA_UID.2, FIA_UAU.2) y política de control de acceso (FDp_ACC.1, FDP_ACF.1). - Generación de auditoría: FAU_GEN.1 y FAU_STG.1 Protección de la traza de auditoría almacenada. FPT_STM.1 Sellados de tiempo fiables

	4. El titular de la autorización deberá disponer de una réplica de su Unidad Central de Apuestas como reserva, preparada para continuar el desarrollo de las apuestas con las mismas condiciones y garantías que la unidad principal en caso de que esta última quede fuera de servicio por cualquier causa.	Dominio SOPORTE • Redundancia y restauración: FRU_FLT.2 Tolerancia a fallos limitada , FPT_RCV.2 Recuperación automática
	5. La Unidad Central de Apuestas, así como su réplica, deberán estar instaladas en el ámbito territorial de la Ciudad de Ceuta y en dependencias bajo el control y la vigilancia de la empresa titular de la autorización.	FOB_BCN.1.1 – Ante la ocurrencia de cualquier evento que ponga en peligro la continuidad del servicio, se garantizará que el personal necesario para garantizar la continuidad estará presente en las instalaciones no más tarde de los 25 minutos posteriores a la ocurrencia del evento.
	6. La Unidad Central de Apuestas incorporará una conexión informática segura y compatible con los sistemas informáticos de la Consejería competente en materia de ordenación y gestión del juego de la Ciudad de Ceuta, para el control y seguimiento en tiempo real de las apuestas, de las cantidades apostadas y de los premios otorgados, así como de la devolución, en su caso, de las apuestas anuladas. Las medidas de seguridad de la conexión deberán garantizar la autenticidad, confidencialidad e integridad en las comunicaciones.	Dominio OPERADORES INTERNOS: • Comunicaciones seguras con los clientes, consejería y otros mercados. FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES Este canal seguro, garantiza autenticación de ambas partes, condifencialidad, integridad.
Artículo 22	4. Las máquinas de apuestas requerirán para su funcionamiento la individualización de una identidad electrónica basada en una firma reconocida, de conformidad con la Ley	• Comunicaciones segurras con las Máquinas de apuestas FTP_ITC.1 Canal seguro Inter-TSF / MÁQUINAS DE APUESTAS En el caso de que la entidad del dominio CLIENTES se corresponda con una “máquina de apuestas”

	59/2003, de Firma Electrónica, y cuya expedición corresponderá al órgano competente, que podrá externalizar este servicio en un Prestador de Servicios de Certificación. La revocación del certificado implicará que la máquina que aloje el dispositivo de creación de firma asociado no podrá prestar sus servicios.	(ver descripción del dominio CLIENTES), el certificado usado en el establecimiento del canal seguro de comunicación con la unidad central, será un certificado reconocido (conforme a la Ley 59/2003, de Firma Electrónica) y cuya expedición corresponderá al órgano competente, que podrá externalizar este servicio en un Prestador de Servicios de Certificación.. La revocación del certificado implicará que la máquina que aloje el dispositivo de creación de firma asociado no podrá prestar sus servicios.
Artículo 23	1. a) Satisfacer los criterios de aleatoriedad en aquellas apuestas en que así se precise. La generación de los datos se realizará de forma aleatoria e imprevisible.	FCS_RNG.1 Generación de números aleatorios (dominio OPERADORES INTERNOS)
Artículo 24	1. Las apuestas podrán formalizarse a través de alguno de los siguientes medios: a) Terminales de expedición y máquinas auxiliares de apuestas, ubicados en los locales y zonas de apuestas. b) Procedimientos informáticos, interactivos o de comunicación a distancia. En este caso, las medidas de seguridad de la conexión correspondiente deberán garantizar la autenticidad del receptor, la confidencialidad y la integridad en las comunicaciones.	Dominio OPERADORES INTERNOS: • Comunicaciones seguras con los clientes, consejería y otros mercados. FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES • Comunicaciones segurras con las Máquinas de apuestas FTP_ITC.1 Canal seguro Inter-TSF / MÁQUINAS DE APUESTAS Estos canales seguros, garantizan autenticación de ambas partes, confidencialidad, integridad.
	2. Las empresas deberán ofrecer a los usuarios la posibilidad de formalizar las apuestas mediante el empleo de la firma electrónica o, en su caso, otros medios análogos que sirvan para acreditar la identidad personal	Dominio clientes: • El registro de clientes FMT_SMF.1 Especificación de las Funciones de Gestión / CLIENTES Podrá ser mediante DNI o formulario.

	del usuario, de conformidad con lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.	• La identificación y autenticación de los clientes (FIA_UID.2, FIA_UAU.2) podrá ser mediante usuario/contraseña o DNIe. Dominio OPERADORES INTERNOS: Para formalizar la apuesta, el cliente deberá hacer un hash y posteriormente firmarla. Esta firma se validará posteriormente en el sistema con el objeto de formalizar la apuesta: • Requisitos de generación de la firma de las apuestas de los clientes: FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS • Se verifica la firma de las apuestas (la del cliente – FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS) y se almacenan los datos garantizando su intergidad (FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS). Se genera el boleto asociado que se envía firmado por la entidad al cliente (FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO). En ese momento se considera formalizada y aceptada la apuesta. Este proceso garantiza el no repudio en ambos lados y la integridad de los datos de las apuestas y boleto almacenados, por lo que se garantiza su trazabilidad.
Artículo 25	1. Sólo se entenderá formalizada válidamente una apuesta de cualquier modalidad cuando se entregue al apostante el boleto o el resguardo acreditativo de la misma expedido por los medios homologados para la realización	Dominio OPERADORES INTERNOS: Para formalizar la apuesta, el cliente deberá hacer un hash y firmarla. Esta firma se validará posteriormente en el sistema con el objeto de formalizar la apuesta. Una vez realizada la validación se emite el boleto firmado.

	de apuestas, o se confirme su validación por medios verificables, ya sean físicos o electrónicos, en el caso de las apuestas realizadas por medios informáticos o electrónicos interactivos. La aceptación de dicho documento por parte del apostante implicará la conformidad con la apuesta realizada. 2. La apuesta se entenderá como no realizada cuando, por causas de fuerza mayor debidamente justificadas, resulte imposible la validación de las mismas.	Los siguientes requisitos demuestran su conformidad: • Requisitos de generación de la firma de las apuestas de los clientes: FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS • Se verifica la firma de las apuestas (la del cliente – FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS) y se almacenan los datos garantizando su intergidad (FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS). Se genera el boleto asociado que se envía firmado por la entidad al cliente (FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO). En ese momento se considera formalizada y aceptada la apuesta. Este proceso garantiza el no repudio en ambos lados y la integridad de los datos de las apuestas y boleto almacenados, por lo que se garantiza su trazabilidad.
Artículo 26	2. El boleto deberá tener el contenido mínimo siguiente: a) Identificación de la empresa autorizada. b) Acontecimiento sobre el que se apuesta y fecha del mismo. c) Modalidad e importe de la apuesta realizada. d) Coeficiente de la apuesta, en su caso. e) Pronóstico realizado. f) Hora, día, mes y año de	Desarrollado como activo del STOE: DATOS_BOLETOS

	formalización de la apuesta. g) Número o combinación alfanumérica que permita identificarlo con carácter exclusivo y único. h) Identificación del medio de formalización de las apuestas utilizado.	
Artículo 28	1. El procedimiento para la formalización de apuestas por medios o sistemas interactivos o de comunicación a distancia deberá desarrollarse en condiciones de seguridad y garantía máximas para el usuario.	Todo el perfil de protección.
	2. La recogida de datos personales, el tratamiento y su utilización posterior deberán sujetarse a la legislación vigente en materia de protección de datos.	[LOPD] FOD_POL.2 Protección de datos y política de privacidad FOA_PRO.1 Privacidad de los datos FOM_CLS.2 Identificación de Activos FOM_PSN.1 Propiedad de los activos
	6. Una vez registradas las apuestas en la Unidad Central, el usuario tendrá derecho a obtener su confirmación electrónica, en la que se refleje, al menos, el contenido mínimo del boleto a que se refiere el artículo 26.2. 7. A efectos de reclamaciones, el sistema de validación aportará toda la información necesaria para identificar y reconstruir de forma fiel la transacción realizada.	Para formalizar la apuesta, el cliente deberá hacer un hash y posteriormente firmarla. Esta firma se validará posteriormente en el sistema con el objeto de formalizar la apuesta: • Requisitos de generación de la firma de las apuestas de los clientes: FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS • Se verifica la firma de las apuestas (la del

		cliente – FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS) y se almacenan los datos garantizando su intergidad (FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS). Se genera el boleto asociado que se envía firmado por la entidad al cliente (FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO). En ese momento se considera formalizada y aceptada la apuesta. Este proceso garantiza el no repudio en ambos lados y la integridad de los datos de las apuestas y boleto almacenados, por lo que se garantiza su trazabilidad. • Requisitos de Auditoría en CLIENTES y OPERADORES FAU_GEN.1 Generación de datos de auditoría / CLIENTES FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES

Justificación de los requisitos funcionales de seguridad

572 Se incluye la justificación los requisitos funcionales de seguridad para el cumplimiento de los objetivos funcionales de seguridad definidos en la sección Objetivos de seguridad funcionales del STOE.

Objetivos Funcionales STOE	Requisitos Funcionales
OF-INT	FTP_ITC.1 Canal seguro Inter-TSF / PASARELA DE PAGO FTP_ITC.1 Canal seguro Inter-TSF / MÁQUINAS DE APUESTAS FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS FCS_CKM.1 Generación de claves criptográficas / FIRMA DEL BOLETO FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES
OF-CONF	**CLIENTES** FIA_UID.2 Identificación de usuario antes de cualquier acción / CLIENTES FIA_UAU.2 Autenticación de usuario antes de cualquier acción / CLIENTES FIA_UAU.5 Mecanismos de autenticación múltiples / CLIENTES FIA_AFL.1 Manejo de fallos de autenticación / CLIENTES FDP_ACC.2 Control de acceso completo / CLIENTES FDP_ACF.1 Atributo de seguridad basado en el control de acceso / CLIENTES FTP_ITC.1 Canal seguro Inter-TSF / PASARELA DE PAGO FTP_ITC.1 Canal seguro Inter-TSF / MÁQUINAS DE APUESTAS

	OPERADORES INTERNOS FIA_UID.2 Identificación de usuario antes de cualquier acción / OPERADORES FIA_UAU.2 Autenticación de usuario antes de cualquier acción / OPERADORES FIA_AFL.1 Manejo de fallos de autenticación / OPERADORES FDP_ACC.2 Control de acceso completo /OPERADORES FDP_ACF.1 Atributo de seguridad basado en el control de acceso /OPERADORES FMT_MSA.1 Gestión de los atributos de seguridad /OPERADORES FMT_MSA.3 Inicialización de atributos estática /OPERADORES FMT_SMR.1 Roles de seguridad/OPERADORES FMT_SMF.1 Especificación de las Funciones de Gestión /OPERADORES FTP_ITC.1 Canal seguro Inter-TSF / CLIENTES Y ENTIDADES **SOPORTE** FIA_UID.2 Identificación de usuario antes de cualquier acción / SOPORTE FIA_UAU.2 Autenticación de usuario antes de cualquier acción / SOPORTE FIA_AFL.1 Manejo de fallos de autenticación / SOPORTE FDP_ACC.2 Control de acceso completo / SOPORTE FDP_ACF.1 Atributo de seguridad basado en el control de acceso / SOPORTE FMT_MSA.1 Gestión de los atributos de seguridad / SOPORTE FMT_MSA.3 Inicialización de atributos estática / SOPORTE FMT_SMR.1 Roles de seguridad/OPERADORES FMT_SMF.1 Especificación de las Funciones de Gestión / SOPORTE FCS_CKM.1 Generación de claves criptográficas / CIFRADO DE DISCOS FCS_CKM.4 Destrucción de claves criptográficas / CIFRADO DE DISCOS FCS_COP.1 Operación criptográfica / CIFRADO DE DISCOS FCS_CKM.1 Generación de claves criptográficas / CIFRADO DE BACKUPS FCS_CKM.4 Destrucción de claves criptográficas / CIFRADO DE BACKUPS FCS_COP.1 Operación criptográfica / CIFRADO DE BACKUPS

	FDP_RIP.1 Protección de un subconjunto de la información residual / BACKUPS
OF-DISP-DATOS	FOS_OAS.2 Procedimientos de copias de respaldo
OF-NOREP-DATOS	FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad / VERIFICACIÓN FIRMA APUESTAS FCS_CKM.1 Generación de claves criptográficas / FIRMA DE LA APUESTA) FCS_COP.1 Operación criptográfica / GENERAR HASH CLIENTE APUESTAS, FCS_COP.1 Operación criptográfica / FIRMAR APUESTAS FCS_COP.1 Operación criptográfica / VERIFICACIÓN FIRMA APUESTAS FCS_COP.1 Operación criptográfica / VERIFICAR HASH CLIENTE APUESTAS FDP_SDI.1 Monitorización de la integridad de los datos almacenados / SERVIDOR APUESTAS FCS_CKM.1 Generación de claves criptográficas / FIRMA DEL BOLETO FCS_COP.1 Operación criptográfica / FIRMA DEL BOLETO
OF-DISP-SERV	FRU_FLT.2 Tolerancia a fallos limitada FPT_RCV.2 Recuperación automática FOS_OAS.2 Procedimientos de copias de respaldo FOS_POL.1 Requisitos de seguridad FOM_PRM.2 Segregación de privilegios FOS_POL.2 Política de código malicioso FOP_RMM.1 Gestión de los Dispositivos Removibles FOP_SYS.1 Gestión del Equipo del Sistema FOP_MNG.1 Seguridad física FOP_MNG.2 Utilidades de apoyo en caso de fallo de corriente
OF-REGISTRO	FMT_SMF.1 Especificación de las Funciones de Gestión / CLIENTES
OF-I&A	FIA_UID.2 Identificación de usuario antes de cualquier acción / CLIENTES FIA_UAU.2 Autenticación de usuario antes de cualquier acción / CLIENTES FIA_UAU.5 Mecanismos de autenticación múltiples / CLIENTES FIA_AFL.1 Manejo de fallos de autenticación / CLIENTES

OF-LOPD	FOS_MON.1 Registros de auditoría FAU_GEN.1 Generación de datos de auditoría / CLIENTES FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES FAU_GEN.1 Generación de datos de auditoría / SOPORTE FAU_STG.1 Protección de la traza de auditoría almacenada / SOPORTE FAU_SAA.1 Análisis de violaciones potenciales FPT_STM.1 Sellados de tiempo fiables FOA_PRO.1 Privacidad de los datos FOA_INF.1 Protección de datos FOD_POL.1 Política de seguridad FOD_POL.2 Protección de datos y política de privacidad FOD_PSN.1 Roles y responsabilidades del personal FOD_RSM.1 Gestión de riesgos de la organización FOM_PRM.2 Segregación de privilegios FOM_CLS.2 Identificación de Activos FOM_PSN.1 Propiedad de los activos FOM_PSN.2 Gestores de seguridad FOM_ORG.1 Responsabilidades de gestión FOD_ORG.1 Responsabilidades de coordinación de seguridad FOS_RCD.1 Registros FOM_INC.1 Informe de los problemas de seguridad detectados
OF-NOEVIL	FOD_PSN.1 Roles y responsabilidades del personal
OF-BCP	FOB_BCN.1 Análisis de impacto FRU_FLT.2 Tolerancia a fallos limitada FPT_RCV.2 Recuperación automática
OF-RND	FCS_RNG.1 Generación de números aleatorios
OF-STAMP	FPT_STM.1 Sellados de tiempo fiables
OF-TRAZA	FAU_GEN.1 Generación de datos de auditoría / CLIENTES FAU_STG.1 Protección de la traza de auditoría almacenada / CLIENTES FAU_GEN.1 Generación de datos de auditoría / OPERADORES FAU_STG.1 Protección de la traza de auditoría almacenada / OPERADORES

Justificación de los requisitos de garantía de seguridad

573 Se incluye la justificación los requisitos de garantía de seguridad para el cumplimiento de los objetivos de garantía de seguridad definidos en la sección Objetivos de seguridad de garantía del STOE.

Objetivo de seguridad	Requisitos de garantía
OA-ASS Declaración de seguridad	ASS_INT.1 ASS_CCL.1 ASS_SPD.1 ASS_OBJ.1 ASS_ECD.1 ASS_REQ.2 ASS_TSS.1 ASS_DMI.1 ASS_DMC.1 ASS_DMP.1 ASS_DMO.1 ASS_DMR.2 ASS_DMS.1
OA-AOD Guías	**Desarrollo e integración** AOD_OCD.1 AOD_OGD.1 **Instalación** AOD_OCD.2 **Operación** AOD_OGD.2 **Modificación** AOD_GVR.2
OA-ASD Desarrollo	**Desarrollo e integración** ASD_SAD.1 ASD_CON.1

	ASD_IFS.1 ASD_STD.1 **Modificación** ASD_RVR.1 ASD_DVR.1
OA-AOC Control de configuración	**Instalación** AOC_OBM.1 AOC_ECP.1 AOC_UCP.1
OA-AOT Pruebas	**Desarrollo e integración** AOT_COV.1 AOT_DPT.1 AOT_FUN.1 **Instalación** AOT_COV.1 AOT_DPT.1 AOT_FUN.1 AOT_IND.1 **Modificación** AOT_REG.1
OA-AOV Análisis de Vulnerabilidades	**Instalación** AOV_VAN.6 **Modificación** AOV_VAN.6
OA-APR	**Instalación**

Preparación del sistema	APR_AWA.1 APR_CMM.1 APR_SIC.1 **Operación** APR_AWA.2 APR_CMM.2 APR_SIC.2
OA-ASO Monitorización	**Operación** ASO_RCD.1 ASO_VER.1 ASO_MON.1

Anejo II. Auditoría de la seguridad.

La auditoría se basará en el análisis de las evidencias existentes que permitan sustentar objetivamente el cumplimento de los requisitos de seguridad especificados en el Reglamento de Apuestas de la Ciudad de Ceuta.

Las actividades que se realizarán en la auditoría se clasifican en:

- Revisión de la documentación de los procedimientos (en el laboratorio).
- Revisión in-situ (ver sección Definición del trabajo técnico) utilizando los siguientes métodos:
    i. Checklist de requisitos
    ii. Pruebas prácticas para la revisión de la implantación y cumplimiento de procedimientos
    iii. Entrevistas (si fuera necesario) al personal afectado

El proyecto tendrá la siguiente planificación de tareas:

A. Plan de auditoría y adaptación de checklists
B. Revisión de documentación de procedimientos de seguridad
C. Realización de revisión in-situ
D. Generación de informes de auditoría

Definición del trabajo técnico

A continuación se detallan las actividades técnicas que se realizarán como parte del proceso de revisión de los procedimientos y pruebas in-situ.

A. Análisis de la política o documento de seguridad

Checklist de cumplimiento de requisitos. Revisión análisis de riesgos.

A1. Análisis del contenido del documento de seguridad.

A2. Control de cambios del documento de seguridad.

A3. Existencia de un análisis de riesgos, con revisión y aprobación anual.

A4. Cumplimiento de los requisitos de la [LOPD] y [RMS] en cuanto al tratamiento de los ficheros con datos de carácter personal con nivel de seguridad BÁSICO.

B. Análisis de los procedimientos de registro de incidencias.

Checklist de cumplimiento de requisitos. Verificación de la implementación del procedimiento.

B 1. Existencia de un procedimiento de notificación y gestión de incidencias. Registro de incidencias: tipo de incidencia, fecha del incidente, persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

B 2. Registro del procedimiento de recuperación de los datos realizado, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

C. Análisis del procedimiento de registro inicial de usuarios.

Verificación de la implementación del procedimiento. Realización de prueba práctica de registro inicial.

C 1. Existencia de un procedimiento de registro de la identidad del usuario.

D. Análisis de los mecanismos de Identificación y autenticación.

Verificación de la implementación del procedimiento. Realización de prueba práctica de I&A con distintos mecanismos.

D 1. Existencia de los siguientes mecanismos de autenticación:

- DNI electrónico (DNIe).
- Registro a través de certificado electrónico reconocido o, en su caso, otros medios análogos que sirvan para acreditar la identidad personal del usuario, de conformidad con lo establecido en la Ley 59/2003, de 19 de diciembre y o posteriores, de Firma Electrónica.

D 2. Existencia de una relación actualizada de usuarios que tengan acceso autorizado al sistema de información por cada fichero. Procedimientos de identificación y autenticación para dicho acceso.

D 3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas

existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

D 4. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

D 5. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

D 6. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

D 7. La aplicación no debe permitir la utilización de claves compartidas o multiusuarios, por tanto la clave debe ser un identificador único, personal e intransferible del usuario.

D 8. La aplicación almacenará las contraseñas mediante mecanismos que garanticen la confidencialidad de las mismas.

D 9. La aplicación no dispondrá de mecanismos que permitan la obtención de la clave del usuario sino la verificación de la misma.

E. Análisis de mecanismos de control de acceso.

Checklist de cumplimiento de requisitos. Verificación de la implementación del procedimiento.

SEGURIDAD FÍSICA

E 1. Checklist para la revisión de los mecanismos de control de acceso en el entorno local y global.

E 2. Revisión de mecanismos de detección de intrusos

SEGURIDAD LÓGICA

E 3. El sistema debe tener un módulo específico para la gestión de administradores del sistema que permita emitir un listado con los usuarios administradores existentes en el mismo. La emisión de los listados sólo podrá ser gestionada por los administradores del sistema para dar cumplimiento a la normativa vigente sobre protección de datos de carácter general.

E 4. El sistema debe disponer de un módulo que permita la gestión de usuarios registrados en el mismo.

E 5. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

E 6. Se establecerán mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

E 7. La relación de usuarios contendrá el acceso autorizado para cada uno de ellos.

E 8. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

E 9. Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal

E 10. Control de acceso en los sistemas informáticos soporte.

F. Análisis del sistema de registro.

Verificación de la implementación del procedimiento. Realización de prueba práctica de generación de registros generales.

F 1. Registro de accesos.

- De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.
- El período mínimo de conservación de los datos registrados será de dos años.
- El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

F 2. Registro de eventos generales

- Emisión de un listado con los usuarios administradores existentes en el mismo.
- El módulo debe permitir al administrador del sistema la obtención de un listado de apuestas.
- El administrador podrá obtener un listado de los movimientos anteriores.

- El sistema deberá disponer de un módulo que permita la generación de un informe mensual que refleje los contenidos establecidos en la Orden EHA/3012/2008, de 20 de octubre.

G. Análisis de los procedimientos de gestión de soportes.

Checklist de cumplimiento de requisitos. Verificación de la implementación del procedimiento.

G 1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

G 2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

G 3. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

G 4. Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

G 5. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

G 6. Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

H. Análisis de los procedimientos de copias de respaldo y recuperación.

Verificación de la implementación del procedimiento. Realización de prueba práctica de recuperación del sistema.

H 1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

H 2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

H 3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

H 4. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

H 5. Con una periodicidad mínima anual se efectuará un procedimiento de recuperación de información salvada con la finalidad de verificar que el proceso de salvado se está efectuando correctamente.

I. Análisis de los sistemas de comunicaciones y garantía de servicio

Checklist de cumplimiento de requisitos. Verificación de la implementación del procedimiento.

I 1. Checklist para revisión de seguridad de redes.

I 2. Garantías del canal de comunicaciones con el usuario final a través del cual se hacen las apuestas y se transmiten datos de carácter personal:

- Autenticación de ambas partes
- Confidencialidad de las apuestas y datos de carácter personal y bancarios
- Integridad de las apuestas y datos de carácter personal y bancarios
- No repudio por ambas partes

I 3. Garantías del canal de comunicaciones con la Consejería competente en materia de ordenación y gestión del juego de la Ciudad Autónoma de Ceuta.

- Autenticación de ambas partes
- Confidencialidad de las apuestas
- Integridad de las apuestas

I 4. Disponibilidad del servicio

- El titular de la autorización debe disponer de una réplica de su Sistema de Apuestas como reserva, preparada para continuar el desarrollo de las apuestas con las mismas condiciones y garantías que el Sistema principal en caso de que este último quede fuera de servicio por cualquier causa.

- Una o varias unidades de la réplica del Sistema de Apuestas podrá estar alojada fuera del territorio de la Ciudad Autónoma de Ceuta con el fin de salvaguardar la misma de cualquier incidente que de forma voluntaria o involuntaria pudiera afectar al perfecto desarrollo y funcionamiento (catástrofe meteorológica, problemas técnicos, tecnológicos, de comunicaciones, etc.).

I 5. Verificación de apuestas y boletos

- El sistema deberá permitir la verificación de cada una de las apuestas formalizadas así como del boleto asociado a las mismas.
- El sistema deberá disponer de mecanismos que garanticen la integridad, el no repudio y la autenticidad de los boletos electrónicos emitidos.
- Sellado de tiempo

I 6. Gestión monetaria

- Confidencialidad de las transacciones
- Integridad de las transacciones
- No repudio por ambas partes

J. Análisis de los procedimientos de continuidad de servicio

Checklist de cumplimiento de requisitos. Verificación de la implementación del procedimiento.

J 1. Análisis de impacto

J 2. Revisión del plan de continuidad de negocio

K. Análisis de vulnerabilidades

Análisis de vulnerabilidades y pruebas de penetración de los componentes o subsistemas de las tecnologías de la información que se intregan para conformar el sistema operacional.