ÁREA D. CONTROLES DE ACCESO A DATOS Y PROGRAMAS

INTRODUCCIÓN

Esta GPF-OCEX 5334 forma parte del conjunto de guías que, junto con la GPF-OCEX 5330 (Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica), están diseñadas para revisar/auditar los CGTI en una entidad que opera en un entorno de administración electrónica avanzada utilizando sistemas de información complejos e interconectados.

En esta guía se aborda la revisión de los controles del área **D. Controles de acceso a datos y programas** y está diseñada para:

- Ayudar a obtener información avanzada sobre el entorno TI de la entidad fiscalizada y de los CGTI.
- Ayudar a identificar riesgos derivados del uso de TI y los CGTI que los aborden.
- Ayudar a evaluar el diseño, implementación y eficacia operativa de los CGTI.
- Ayudar a identificar la existencia de deficiencias en esos controles que puedan derivar en riesgos significativos.
- Documentar los procedimientos llevados a cabo, la evidencia obtenida y las conclusiones alcanzadas respecto al diseño, implementación y eficacia operativa de los CGTI.

Tal y como se indica en GPF-OCEX 5330 (apartado 14), **los controles de esta área son importantes** por los siguientes motivos:

> *"Esta área incluye todos aquellos controles relativos a la gestión de usuarios, sus privilegios y los mecanismos de identificación y autenticación. Estos controles son principalmente organizativos y de gestión, y por su especial relevancia deben encontrarse expresamente recogidos en las políticas y normas de seguridad de la organización.*
>
> *Los controles de acceso son importantes por dos motivos principales.*
>
> *El primero motivo es que los usuarios son, probablemente, el vector de ataque más importante de las amenazas existentes y su acceso y gestión deben encontrarse especialmente protegidos. Las amenazas sobre los usuarios pueden ser de naturaleza fortuita, por un uso inadecuado de sistemas o privilegios por parte de usuarios legítimos. O intencional, debido a amenazas externas que explotan la configuración inadecuada de los mecanismos de acceso, identificación y gestión de usuarios y privilegios de los sistemas.*
>
> *El segundo motivo es el especial impacto de los controles del área sobre los CPI de los sistemas. Los controles de acceso son condición indispensable para permitir el adecuado funcionamiento de CPI esenciales, como por ejemplo los controles de segregación de funciones."*

El contenido de la presente guía, con carácter general, no debe ser considerado para su aplicación de manera exhaustiva. Tal y como se indica en el apartado 2 de la GPF-OCEX 5330, únicamente se deberán evaluar aquellos controles identificados que sean relevantes o significativos, en función de los objetivos y alcance de la auditoría que se esté realizando.

Una vez identificados los controles relevantes, se deberá realizar una selección de los procedimientos de auditoría de las guías 5331 a 5335 correspondientes a estos controles relevantes, incluyendo aspectos a evaluar, preguntas, propuesta de evidencias, etc. Este subconjunto de procedimientos constituirá el programa de trabajo de cada auditoría en particular.

Tal y como se indica en la guía GPF-OCEX 5330, el conjunto de guías de esta serie mantiene "*la máxima coherencia con los postulados del ENS, puesto que es de obligado cumplimiento para todos los entes públicos y esta alineación facilita la realización de las auditorías de CGTI y coadyuvan a la implantación del ENS*". El contenido de esta guía ha sido desarrollado utilizando como base la "Guía de Seguridad de las TIC CCN-STIC 808" y, aunque se han incluido determinadas modificaciones y ampliaciones sobre los procedimientos de revisión, mantiene total compatibilidad con la guía STIC.

D1 – USO CONTROLADO DE PRIVILEGIOS DE ADMINISTRACIÓN

D.1.1: Inventario y control de cuentas de administración

Los privilegios de administración están limitados adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita su correcto control.

Requisitos:

op.acc.1.3	Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de estos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.
op.acc.2.3	Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.
op.acc.3.r3.1	El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Propuesta de evidencias:

	☐	Procedimiento de gestión de cuentas de administración.
	☐	Formalización de la responsabilidad de administración del sistema TI (por ejemplo, responsabilidades del puesto en la RPT, documentación interna de organización del departamento de TI, etc.).
	☐	Inventario de cuentas de administración para los distintos sistemas o evidencia del listado de usuarios con privilegios de administración para cada uno de los sistemas analizados
	☐	Documentación de seguridad del sistema, en la que se describa el sistema de identificación utilizado en cada sistema.
	☐	Fichero de usuarios obtenido directamente de cada uno los sistemas bajo análisis.
	☐	Evidencia del cambio de contraseña de las cuentas de administración compartidas tras el cese de uno de los administradores.
	☐	Evidencia de deshabilitación de las cuentas y su control hasta su eliminación definitiva.
	☐	Evidencia de uso herramientas para el almacenamiento cifrado y el control de acceso a las contraseñas de uso compartido (tipo *Keepass*).
	☐	Evidencia de soluciones PAM (*Privileged Account Management*) para la gestión de las cuentas de administración.
	☐	Evidencias sobre qué mecanismos de acceso al sistema en modo administrador ha establecido la entidad y cómo ha implantado este control.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Está adecuadamente controlada la asignación del privilegio de administración?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	¿Está formalizada la asignación de privilegios de administración?
	¿Hay un proceso establecido para la asignación de privilegios de administración? *NOTA: Para verificar la efectiva implantación de este proceso, obtener el inventario de cuentas de administración (si se tiene) y compararlo con los usuarios administradores dados de alta en cada uno de los sistemas bajo análisis. Comprobar que corresponden al personal activo de la entidad.*
N2	¿Está documentado?
N0	Cuando un miembro del departamento de informática abandona el departamento, ¿se le dan de baja los privilegios de administración? *NOTA: Para verificar la efectiva implantación de este proceso, obtener la relación de usuarios que disponen del privilegio de administración en cada uno de los sistemas y compararlo con el inventario (si se tiene) de usuarios administradores autorizados.*
	Una vez deja de ser necesaria una cuenta, ¿se retiene deshabilitada durante un período finito y determinado para atender a las necesidades de trazabilidad de los registros asociados a la misma, antes de su eliminación?
N0	Cuando un miembro del departamento de informática abandona el departamento, ¿se cambian las contraseñas de los usuarios de administración compartidos a los que hubiese tenido acceso la persona que causa la baja?
N0	**Los usuarios utilizados para la administración de sistemas, ¿permiten mantener la trazabilidad de las acciones realizadas con estas cuentas?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se utilizan las cuentas de administración por defecto del sistema TI?
	Tanto si se utilizan las cuentas de administración por defecto como si se han creado otras cuentas con privilegios de administración ¿se comparten estas cuentas?
	En caso afirmativo, ¿la gestión de la contraseña de acceso impide accesos no autorizados o uso no autorizado de estos privilegios?
	En caso de uso compartido de cuentas de administración, ¿se dispone de algún control, manual o automático, que permita saber quién ha realizado una acción? (por ejemplo, quién ha iniciado sesión y modificado un parámetro si el usuario que aparece en el log es "root"). *Nota: Considerar opciones como el uso de sudo, de la opción "run as", etc.*
	La entidad utiliza algún producto de tipo PAM (*Privileged Account Management*).
	¿Se controlan las cuentas con privilegios y los mecanismos desde los cuales pueden acceder a la administración de los sistemas?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.1.2: Uso dedicado de cuentas de administración

Las cuentas de administración sólo se utilizan para las tareas que son estrictamente necesarias.

Requisitos:

Op.acc.1.2	Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

Propuesta de evidencias:

	☐	Listado del personal que tiene asignado el privilegio de administración (en la mayoría de los casos serán miembros del departamento TI de la entidad y de proveedores que les den soporte).
	☐	Evidencia del uso por parte del personal que realiza labores de administración de diferentes cuentas de usuario, según vayan a realizar labores de administración o tareas rutinarias que no requieran este privilegio.
	☐	Documentación de seguridad del sistema, en la que se describa el sistema de identificación utilizado en cada sistema.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Cuando el usuario tiene diferentes roles frente al sistema, ¿se le asignan identificadores singulares para cada perfil, de forma que se recaben los correspondientes registros de actividad en base a los privilegios correspondientes a cada perfil para poder conocer las acciones realizadas?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	El personal que dispone de dos cuentas de acceso al sistema, una con privilegios de administración y otra sin ellos, ¿utiliza esta última para todas aquellas acciones que no requieren de dicho privilegio? NOTA: Para evidenciar esta cuestión, se puede comprobar, por ejemplo, con qué cuenta se inicia diariamente la sesión en el equipo de usuario al inicio de la jornada laboral (debería ser la del usuario que no dispone de privilegios de administración).

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.1.3: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización

Las cuentas de administración utilizadas por personal interno de la entidad están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.

Requisitos:

Op.acc.6	Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.
6.1	- Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.
6.2	- Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia.
6.3	- Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
6.4	- Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad.
6.5	- Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a terceros no autorizados.
6.6	- Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.
6.7	- Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo.
6.8	- El número de intentos permitidos será limitado, bloqueando el acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
6.9	- El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.
op.acc.6.r5.1	- Se registrarán los accesos con éxito y los fallidos.
op.acc.6.r5.2	- Se informará al usuario del último acceso efectuado con su identidad.
op.acc.6.r6.1	- Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.
op.acc.6.r7.1	- Las credenciales se suspenderán tras un periodo definido de no utilización.
op.acc.6.r8.1	- Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación. Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.
op.acc.6.r9.2	El acceso remoto deberá considerar los siguientes aspectos: a) Ser autorizado por la autoridad correspondiente. b) El tráfico deberá ser cifrado. c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario. d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Propuesta de evidencias*:*

	☐	Documentación de seguridad del sistema, en la que se describa las características del mecanismo de autenticación de cada sistema, incluyendo los criterios específicos para usuarios administradores (si aplica).
	☐	Evidencia de la política de autenticación implantada en cada sistema para los usuarios administradores.
	☐	Evidencia del proceso de entrega y aceptación de credenciales por los usuarios.
	☐	Evidencia de deshabilitación / retirada de credenciales a los usuarios.
	☐	Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible.
	☐	Evidencia de doble factor de autenticación.
	☐	Evidencia de empleo de contraseñas de un solo uso (OTP).
	☐	Evidencia de que los certificados empleados son cualificados.
	☐	Evidencia de que se configuran los certificados protegidos mediante un segundo factor (p.ej. PIN).
	☐	Evidencias de registros de acceso.
	☐	Evidencia de que se informa al usuario del último acceso.
	☐	Evidencia de que para el acceso remoto se requiere autorización específica, se cifra su tráfico, se recogen pistas de auditoría y es deshabilitado fuera de los períodos establecidos de utilización.
	☐	Evidencia de acceso, mediante cuentas de administración, únicamente desde determinados dispositivos.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿La política de autenticación para los <u>usuarios administradores correspondientes a personal de la entidad</u> se considera robusta y adecuada para reducir el riesgo de accesos no autorizados?**
	• **Posibles mecanismos de autenticación contemplados en el ENS son: contraseñas, certificados y certificados cualificados.**
	• **Medidas que incrementan la robustez de la autenticación:**
	  ○ **Doble factor de autenticación**
	  ○ **Protección del uso de certificados mediante un segundo factor de autenticación.**
	
	☐ SI ☐ NO

Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	Si se utilizan contraseñas, estas consideran: Vigencia máxima, vigencia mínima, Longitud mínima, complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales) e histórico de contraseñas recordadas.
N0	¿Se dispone de bloqueo de la cuenta tras intentos reiterados de acceso fallidos? Cuando la cuenta se bloquea, ¿permanece bloqueada hasta que sea reactivada por un administrador?

NOTA:

- *Cat. BÁSICA: Cumplir, al menos, con uno de los refuerzos R1, R2, R3 o R4 y siempre con R8 y R9;*
- *Cat. MEDIA: Cumplir con una de las medidas R1, R2, R3 o R4 y siempre con R5, R8 y R9;*
- *Cat. ALTA Cumplir con una de las medidas R1, R2, R3, o R4 y siempre con R5, R6, R7, R8 y R9.*

N0	**R1. ¿Se emplea una contraseña como mecanismo de autenticación, con garantías razonables?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	Si se emplea una contraseña como mecanismo de autenticación, ¿se verifica que el acceso se realiza únicamente desde zonas controladas y sin atravesar zonas no controladas?
N0	Si se emplean contraseñas o similares, ¿se imponen normas de longitud, complejidad mínima y robustez, frente a ataques de adivinación?
N0	**R2. ¿Se requiere un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es»?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	**R3. ¿Se emplean certificados cualificados como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se encuentra protegido el uso del certificado mediante un segundo factor, del tipo PIN o biométrico?
N0	**R4. ¿Se emplean certificados cualificados en soporte físico (tarjeta o similar) como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se encuentra protegido el uso del certificado mediante un segundo factor, del tipo PIN o biométrico?
N0	**R8. ¿Se requiere un doble factor de autenticación para el acceso desde zonas no controladas?** ☐ SI ☐ NO *NOTA: Se entiende por zona controlada aquella que no es de acceso público, sino que para llegar al equipo desde el que se accede, el usuario se ha identificado de alguna forma (control de acceso a las instalaciones) diferente al mecanismo de autenticación lógica frente al sistema*.
	Espacio disponible para la redacción de la respuesta
N0	**R9. Respecto a los accesos remotos ¿Se contemplan aspectos de seguridad y autorización?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Los accesos remotos son autorizados por la autoridad correspondiente en la organización?
N0	¿Está cifrado el tráfico de los accesos remotos?
N0	**R5. ¿Se registran las trazas de acceso y se informa de la más reciente al usuario?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se registran tanto los accesos fallidos, como los que han tenido éxito?
	¿Se informa al usuario del último acceso realizado con su identidad?
N0	**¿Se dispone de un proceso para la gestión de la activación del mecanismo de autenticación (por ejemplo, credenciales)?** *Nota: La entrega de credenciales al personal administrador no es una casuística que, a priori, presente riesgo alto específico. No obstante, el ENS requiere implantar este control para la totalidad de usuarios. Por ello y por los casos en los que se considere necesaria la revisión, se incluye a continuación el cuestionario de revisión.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	¿Se activan las credenciales únicamente cuando éstas están bajo el control exclusivo y efectivo del usuario, o se fuerza un cambio de credenciales al primer acceso?
	Antes de proporcionar las credenciales a los usuarios, ¿estos han conocido y aceptado la política de seguridad del organismo en los aspectos que les afecten?
	¿Reconoce el usuario que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida?
N0	¿Se cambian las credenciales con la periodicidad marcada por la política de la organización?
N0	¿Se retiran y deshabilitan las credenciales cuando la persona que se autentica termina su relación con el sistema?
N0	¿Se deshabilitan o regeneran las credenciales cuando se detecta o sospecha su pérdida o revelación a personas no autorizadas?
	¿Se previenen ataques que puedan revelar información del sistema sin llegar a acceder al mismo? ¿la información suministrada en los accesos se restringe a la mínima imprescindible?
	¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener éste el acceso?

Procedimientos de auditoría

- Revisar la política de autenticación que aplica a los usuarios administradores de cada uno de los sistemas incluidos en el alcance.
- Revisar la política de bloqueo de cuentas que aplica a los usuarios administradores de cada uno de los sistemas incluidos en el alcance.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.1.4: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos

Las cuentas de administración utilizadas por usuarios externos a la entidad están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.

Requisitos:

Op.acc.5.1	- Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.
Op.acc.5.2	- Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia.
Op.acc.5.3	- Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
Op.acc.5.4	- Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad.
Op.acc.5.5	- Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a terceros no autorizados.
Op.acc.5.6	- Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
Op.acc.5.7	- Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible, evitando todo aquello que pueda revelar información sobre el sistema. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.
Op.acc.5.8	- El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
Op.acc.5.9	- El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.
op.acc.5.r5.1	- Se registrarán los accesos con éxito y los fallidos.
op.acc.5.r5.2	- Se informará al usuario del último acceso efectuado con su identidad.
op.acc.5.r6.1	- Se definirán los puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.
op.acc.5.r7.1	- Las credenciales se suspenderán tras un periodo definido de no utilización.

Propuesta de evidencias*:*

	☐	Documentación de seguridad del sistema, en la que se describa las características del mecanismo de autenticación de cada sistema, incluyendo los criterios específicos para usuarios administradores (si aplica).
	☐	Evidencia de la política de autenticación implantada en cada sistema para los usuarios administradores.
	☐	Evidencia del proceso de entrega y aceptación de credenciales por los usuarios.
	☐	Evidencia de deshabilitación / retirada de credenciales a los usuarios.
	☐	Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	☐	Evidencia de empleo de contraseñas de un solo uso (OTP).
	☐	Evidencia de que los certificados empleados son cualificados.
	☐	Evidencia de que se configuran los certificados protegidos mediante un segundo factor (p.ej. PIN).
	☐	Evidencia de empleo de certificados cualificados en soporte físico, protegidos mediante un segundo factor.
	☐	Evidencia de que el sistema registra los accesos con éxito y los fallidos.
	☐	Evidencia de que se informa al usuario del último acceso efectuado con su identidad.
	☐	Evidencia de suspensión de las credenciales tras un período definido de no utilización.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿La política de autenticación para los <u>usuarios administradores utilizados por personal externo</u> se considera robusta y adecuada para reducir el riesgo de accesos no autorizados?** • **Posibles mecanismos de autenticación contemplados en el ENS son: contraseñas, certificados y certificados cualificados.** • **Medidas que incrementan la robustez de la autenticación:** ○ **Doble factor de autenticación** ○ **Protección del uso de certificados mediante un segundo factor de autenticación.** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	Si se utilizan contraseñas, estas consideran: Vigencia máxima, vigencia mínima, Longitud mínima, complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales) e histórico de contraseñas recordadas.
N0	¿Se dispone de bloqueo de la cuenta tras intentos reiterados de acceso fallidos? Cuando la cuenta se bloquea, ¿permanece bloqueada hasta que sea reactivada por un administrador?
NOTA: - *Cat. BÁSICA y MEDIA: Cumplir, al menos con uno de los refuerzos R1, R2, R3 o R4.* - *Cat. ALTA: Cumplir con R2 o R3 o R4 y siempre con R5.*	
N0	**R1. ¿Se emplea una contraseña como mecanismo de autenticación, con garantías razonables?** ☐ SI ☐ NO
N0	**R2. ¿Se requiere una contraseña de un solo uso (OTP) como complemento a la contraseña de usuario?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**R3. ¿Se emplean certificados cualificados como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se le facilitan las credenciales al usuario tras un registro previo, presencial o telemático, usando certificado electrónico cualificado?
N0	¿El uso del certificado está protegido por un segundo factor, del tipo PIN o biométrico?
N0	**R4 ¿Se emplean certificados cualificados en soporte físico (tarjeta o similar) como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Los certificados emplean algoritmos, parámetros y dispositivos autorizados por el CCN? NOTA: Se relacionan en la guía CCN-STIC 807 sobre Criptología de empleo en el ENS.
N0	¿Se le facilitan las credenciales al usuario tras un registro previo, presencial o telemático, usando certificado electrónico cualificado?
N0	¿El uso del certificado está protegido por un segundo factor, del tipo PIN o biométrico?
N0	**R5. ¿Se registran los accesos, o su intento, y se informa al usuario?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿El sistema registra los accesos con éxito y los fallidos?
	¿Se le informa al usuario del último acceso efectuado con su identidad?
	R7 ¿Se suspenden las credenciales tras un periodo definido de no utilización? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**¿Se mantiene la seguridad de las cuentas y las credenciales de los usuarios externos, mediante mecanismos de control de acceso?** *Nota: La entrega de credenciales al personal administrador no es una casuística que, a priori, presente riesgo alto específico. No obstante, el ENS requiere implantar este control para la totalidad de usuarios. Por ello y por los casos en los que se considere necesaria la revisión, se incluye a continuación el cuestionario de revisión.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se activan las credenciales únicamente cuando éstas están bajo el control exclusivo y efectivo del usuario, o se fuerza un cambio de credenciales al primer acceso?
	Antes de activar el mecanismo de autenticación, ¿el usuario reconoce que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia?
	Antes de proporcionar las credenciales de autenticación a las entidades, ¿se identifican y registran éstos previamente de manera fidedigna ante el sistema, ante un Prestador Cualificado de Servicios de Confianza, o en un proveedor de identidad electrónica? *NOTA: Dicho proveedor ha de ser reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.*
	¿Se dispone de evidencias de que el usuario reconoce que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida?
N0	¿Se retiran y deshabilitan las credenciales cuando se detecta su pérdida o falta de control exclusivo por parte del usuario?
N0	¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que se autentica termina su relación con el sistema?
	¿La información suministrada en los accesos se restringe a la mínima imprescindible? NOTA: Se evita todo aquello que pueda revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo
N0	¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener éste el acceso?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D2 – GESTIÓN DE USUARIOS

D.2.1: Procedimiento de gestión de usuarios

La entidad dispone de un procedimiento para la gestión de los usuarios de los sistemas y los derechos de acceso asignados a cada uno.

Requisitos:

op.acc.1.4	Las cuentas de usuario se gestionarán de la siguiente forma: a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único. b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario. c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».
[op.acc.1.r1.3]	Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.
op.acc.4.4	–Los permisos de acceso se revisarán de forma periódica.

Propuesta de evidencias:

	☐	Procedimiento de gestión de solicitud y alta de nuevos usuarios en los sistemas.
	☐	Evidencias de solicitud de alta de nuevos usuarios en el sistema y evidencia de la autorización dada para la creación de estas altas.
	☐	Procedimiento de baja de usuarios.
	☐	Evidencia de deshabilitación de cuentas y su control hasta la supresión definitiva.
	☐	Relación facilitada por el personal del departamento de RRHH de altas, bajas y cambios de puesto registrados durante el periodo auditado.
	☐	Relación de cuentas activas en cada sistema TI que permita comprobar que estas responden a necesidades vigentes.
	☐	Procedimiento de revisión de usuarios y privilegios.
	☐	Evidencias de ejecución de revisiones de usuarios y privilegios realizadas.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	***¿Dispone la entidad de un proceso formalmente establecido de solicitud y alta de nuevos usuarios en los sistemas?*** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	¿Está documentado el proceso de gestión de solicitud y alta de nuevos usuarios?
	El procedimiento de gestión de usuarios, ¿incluye la gestión de usuarios administradores?
	¿Están asignadas claramente las responsabilidades asociadas a la creación de nuevas cuentas de usuario en el sistema (como mínimo, quién debe autorizar)?
N0/N2	***¿Dispone la entidad de un proceso formalmente establecido para la gestión de las bajas de cuentas de usuarios en el sistema que garantice que no existen cuentas no necesarias?*** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	Si un usuario causa baja en la entidad, ¿se bloquea inmediatamente el usuario de acceso? *NOTA: comprobar que se cumple lo anterior mediante el análisis de la fecha de última conexión al sistema de cada uno de los usuarios activos.*
	Si un usuario causa baja en la entidad, ¿se mantiene la cuenta durante el periodo de retención definido?
	Si un usuario cesa en su responsabilidad, ¿se bloquean inmediatamente los privilegios que ya no son necesarios? *NOTA: comprobar que se cumple lo anterior mediante la revisión de una muestra de usuarios que hayan cambiado de puesto.*
N0	***¿Dispone la entidad de un proceso formalmente establecido de revisión de usuarios existentes?*** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se realizan revisiones de usuarios que permitan identificar cuentas de acceso no necesarias?
N0	¿Se realizan revisiones de privilegios asociados a usuarios que permitan identificar privilegios no necesarios?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.2.2: Identificación

Se utiliza la identificación singular de usuarios para gestionar el acceso a los sistemas.

Requisitos:

[op.acc.1.1] op.acc.1.2 op.acc.1.3 op.acc.1.4	La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación: – Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema recogidos en la Ley 39/2015, de 1 de octubre. – Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil. – Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad. a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

Propuesta de evidencias:

	☐	Evidencia de métodos de identificación.
	☐	Normativa de construcción del identificador de usuario.
	☐	Listado de usuarios de cada sistema.
	☐	Relación de los usuarios que disponen de más de un rol e identificadores asociados a cada uno de los roles.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Cada entidad (entidad, usuario o proceso) que accede al sistema, ¿cuenta con un identificador singular que permita conocer el destinatario y asignarle los derechos de acceso que le correspondan?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	Antes de asignar un identificador para el acceso a los sistemas, ¿se comprueba la identidad de la persona?
N0	¿Todos los usuarios existentes en los sistemas son singulares? *NOTA: Para ello, obtener la relación de usuarios de los sistemas bajo análisis y comprobar que no existen cuentas genéricas o que no siguen el patrón de construcción del identificador de usuario recogido en la normativa.*
	Cuando el usuario tiene diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo), ¿se le asignan identificadores singulares para cada perfil?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.2.3: Mecanismos de autenticación (usuarios internos)

Las cuentas utilizadas por personal interno de la entidad están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.

Requisitos:

Op.acc.6	Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.
6.1	- Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.
6.2	- Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia.
6.3	- Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
6.4	- Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad.
6.5	- Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a terceros no autorizados.
6.6	- Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.
6.7	- Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema. Las credenciales solamente se validarán
6.8	cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo. - El número de intentos permitidos será limitado, bloqueando el acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá
6.9	en la documentación. - El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de
op.acc.6.r5.1	obtener el acceso.
op.acc.6.r5.2	- Se registrarán los accesos con éxito y los fallidos.
op.acc.6.r6.1	- Se informará al usuario del último acceso efectuado con su identidad. - Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión
op.acc.6.r7.1	establecida.
op.acc.6.r8.1	- Las credenciales se suspenderán tras un periodo definido de no utilización.
op.acc.6.r9.2	- Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación. Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet. El acceso remoto deberá considerar los siguientes aspectos: a) Ser autorizado por la autoridad correspondiente. b) El tráfico deberá ser cifrado. c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario. d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Propuesta de evidencias*:*

	☐	Documentación de seguridad del sistema, en la que se describa las características del mecanismo de autenticación de cada sistema, incluyendo los criterios específicos para usuarios administradores (si aplica).
	☐	Evidencia de la política de autenticación implantada en cada sistema para los usuarios administradores.
	☐	Evidencia del proceso de entrega y aceptación de credenciales por los usuarios.
	☐	Evidencia de deshabilitación / retirada de credenciales a los usuarios.
	☐	Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible.
	☐	Evidencia de doble factor de autenticación.
	☐	Evidencia de empleo de contraseñas de un solo uso (OTP).
	☐	Evidencia de que los certificados empleados son cualificados.
	☐	Evidencia de que se configuran los certificados protegidos mediante un segundo factor (p.ej. PIN).
	☐	Evidencias de registros de acceso.
	☐	Evidencia de que se informa al usuario del último acceso.
	☐	Evidencia de que para el acceso remoto se requiere autorización específica, se cifra su tráfico, se recogen pistas de auditoría y es deshabilitado fuera de los períodos establecidos de utilización.
	☐	Evidencia de acceso, mediante cuentas de administración, únicamente desde determinados dispositivos.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿La política de autenticación se considera robusta y adecuada para reducir el riesgo de accesos no autorizados?** • **Posibles mecanismos de autenticación contemplados en el ENS son: contraseñas, certificados y certificados cualificados.** • **Medidas que incrementan la robustez de la autenticación:** ○ **Doble factor de autenticación** ○ **Protección del uso de certificados mediante un segundo factor de autenticación.** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
N0	Si se utilizan contraseñas, estas consideran: Vigencia máxima, vigencia mínima, Longitud mínima, complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales) e histórico de contraseñas recordadas.
N0	¿Se dispone de bloqueo de la cuenta tras intentos reiterados de acceso fallidos? Cuando la cuenta se bloquea, ¿permanece bloqueada hasta que sea reactivada por un administrador?
NOTA: • *Cat. BÁSICA: Cumplir, al menos, con uno de los refuerzos R1, R2, R3 o R4 y siempre con R8 y R9;* • *Cat. MEDIA: Cumplir con una de las medidas R1, R2, R3 o R4 y siempre con R5, R8 y R9;* • *Cat. ALTA Cumplir con una de las medidas R1, R2, R3, o R4 y siempre con R5, R6, R7, R8 y R9.*	
N0	**R1. ¿Se emplea una contraseña como mecanismo de autenticación, con garantías razonables?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
N0	Si se emplea una contraseña como mecanismo de autenticación, ¿se verifica que el acceso se realiza únicamente desde zonas controladas y sin atravesar zonas no controladas?
N0	Si se emplean contraseñas o similares, ¿se imponen normas de longitud, complejidad mínima y robustez, frente a ataques de adivinación?
N0	**R2. ¿Se requiere un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es»?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**R3. ¿Se emplean certificados cualificados como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se encuentra protegido el uso del certificado mediante un segundo factor, del tipo PIN o biométrico?
N0	**R4. ¿Se emplean certificados cualificados en soporte físico (tarjeta o similar) como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se encuentra protegido el uso del certificado mediante un segundo factor, del tipo PIN o biométrico?
N0	**R8. ¿Se requiere un doble factor de autenticación para el acceso desde zonas no controladas?** ☐ SI ☐ NO *NOTA: Se entiende por zona controlada aquella que no es de acceso público, sino que para llegar al equipo desde el que se accede, el usuario se ha identificado de alguna forma (control de acceso a las instalaciones) diferente al mecanismo de autenticación lógica frente al sistema. Es decir, cualquier zona que está fuera de las instalaciones/red de la organización.*
	Espacio disponible para la redacción de la respuesta
N0	**R9. Respecto a los accesos remotos ¿Se contemplan aspectos de seguridad y autorización?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Los accesos remotos son autorizados por la autoridad correspondiente en la organización?
N0	¿Está cifrado el tráfico de los accesos remotos?
N0	**R5. ¿Se registran las trazas de acceso y se informa de la más reciente al usuario?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se registran tanto los accesos fallidos, como los que han tenido éxito?
	¿Se informa al usuario del último acceso realizado con su identidad?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**¿Se dispone de un proceso para la gestión de la activación del mecanismo de autenticación (por ejemplo, credenciales)?** *Nota: La entrega de credenciales en entidades pequeñas con poca o ninguna dispersión geográfica no es una casuística que, a priori, presente riesgo alto específico. No obstante, el ENS requiere implantar este control para la totalidad de usuarios y en cualquier circunstancia. Por ello y por los casos en los que se considere necesaria la revisión, se incluye a continuación el cuestionario de revisión.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se activan las credenciales únicamente cuando éstas están bajo el control exclusivo y efectivo del usuario, o se fuerza un cambio de credenciales al primer acceso?
	Antes de proporcionar las credenciales a los usuarios, ¿estos han conocido y aceptado la política de seguridad del organismo en los aspectos que les afecten?
	¿Reconoce el usuario que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida?
N0	¿Se cambian las credenciales con la periodicidad marcada por la política de la organización?
N0	¿Se retiran y deshabilitan las credenciales cuando la persona que se autentica termina su relación con el sistema?
N0	¿Se deshabilitan o regeneran las credenciales cuando se detecta o sospecha su pérdida o revelación a personas no autorizadas?
	¿Se previenen ataques que puedan revelar información del sistema sin llegar a acceder al mismo? ¿la información suministrada en los accesos se restringe a la mínima imprescindible?
	¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener éste el acceso?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.2.4: Mecanismos de autenticación (usuarios externos)

Las cuentas de usuarios externos están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.

Requisitos:

Op.acc.5.1	- Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.
Op.acc.5.2	- Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia.
Op.acc.5.3	- Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
Op.acc.5.4	- Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad.
Op.acc.5.5	- Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a terceros no autorizados.
Op.acc.5.6	- Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
Op.acc.5.7	- Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible, evitando todo aquello que pueda revelar información sobre el sistema. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.
Op.acc.5.8	- El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
Op.acc.5.9	- El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.
op.acc.5.r5.1	- Se registrarán los accesos con éxito y los fallidos.
op.acc.5.r5.2	- Se informará al usuario del último acceso efectuado con su identidad.
op.acc.5.r6.1	- Se definirán los puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.
op.acc.5.r7.1	- Las credenciales se suspenderán tras un periodo definido de no utilización.

Propuesta de evidencias*:*

	☐	Documentación de seguridad del sistema, en la que se describa las características del mecanismo de autenticación de cada sistema, incluyendo los criterios específicos para usuarios administradores (si aplica).
	☐	Evidencia de la política de autenticación implantada en cada sistema para los usuarios administradores.
	☐	Evidencia del proceso de entrega y aceptación de credenciales por los usuarios.
	☐	Evidencia de deshabilitación / retirada de credenciales a los usuarios.
	☐	Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible.
	☐	Evidencia de empleo de contraseñas de un solo uso (OTP).

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	☐	Evidencia de que los certificados empleados son cualificados.
	☐	Evidencia de que se configuran los certificados protegidos mediante un segundo factor (p.ej. PIN).
	☐	Evidencia de empleo de certificados cualificados en soporte físico, protegidos mediante un segundo factor.
	☐	Evidencia de que el sistema registra los accesos con éxito y los fallidos.
	☐	Evidencia de que se informa al usuario del último acceso efectuado con su identidad.
	☐	Evidencia de suspensión de las credenciales tras un período definido de no utilización.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿La política de autenticación para los usuarios administradores se considera robusta y adecuada para reducir el riesgo de accesos no autorizados?** • **Posibles mecanismos de autenticación contemplados en el ENS son: contraseñas, certificados y certificados cualificados.** • **Medidas que incrementan la robustez de la autenticación:** ○ **Doble factor de autenticación** ○ **Protección del uso de certificados mediante un segundo factor de autenticación.** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	Si se utilizan contraseñas, estas consideran: Vigencia máxima, vigencia mínima, Longitud mínima, complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales) e histórico de contraseñas recordadas.
N0	¿Se dispone de bloqueo de la cuenta tras intentos reiterados de acceso fallidos? Cuando la cuenta se bloquea, ¿permanece bloqueada hasta que sea reactivada por un administrador?
NOTA: - *Cat. BÁSICA y MEDIA: Cumplir, al menos con uno de los refuerzos R1, R2, R3 o R4.* - *Cat. ALTA: Cumplir con R2 o R3 o R4 y siempre con R5.*	
N0	**R1. ¿Se emplea una contraseña como mecanismo de autenticación, con garantías razonables?** ☐ SI ☐ NO
N0	**R2. ¿Se requiere una contraseña de un solo uso (OTP) como complemento a la contraseña de usuario?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**R3. ¿Se emplean certificados cualificados como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se le facilitan las credenciales al usuario tras un registro previo, presencial o telemático, usando certificado electrónico cualificado?
N0	¿El uso del certificado está protegido por un segundo factor, del tipo PIN o biométrico?
N0	**R4 ¿Se emplean certificados cualificados en soporte físico (tarjeta o similar) como mecanismo de autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Los certificados emplean algoritmos, parámetros y dispositivos autorizados por el CCN? NOTA: Se relacionan en la guía CCN-STIC 807 sobre Criptología de empleo en el ENS.
N0	¿Se le facilitan las credenciales al usuario tras un registro previo, presencial o telemático, usando certificado electrónico cualificado?
N0	¿El uso del certificado está protegido por un segundo factor, del tipo PIN o biométrico?
N0	**R5. ¿Se registran los accesos, o su intento, y se informa al usuario?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿El sistema registra los accesos con éxito y los fallidos?
	¿Se le informa al usuario del último acceso efectuado con su identidad?
	R7 ¿Se suspenden las credenciales tras un periodo definido de no utilización? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**¿Se mantiene la seguridad de las cuentas y las credenciales de los usuarios externos, mediante mecanismos de control de acceso?** *Nota: La entrega de credenciales en entidades pequeñas con poca o ninguna dispersión geográfica no es una casuística que, a priori, presente riesgo alto específico. No obstante, el ENS requiere implantar este control para la totalidad de usuarios y en cualquier circusntancia. Por ello y por los casos en los que se considere necesaria la revisión, se incluye a continuación el cuestionario de revisión.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se activan las credenciales únicamente cuando éstas están bajo el control exclusivo y efectivo del usuario, o se fuerza un cambio de credenciales al primer acceso?
	Antes de activar el mecanismo de autenticación, ¿el usuario reconoce que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia?
	Antes de proporcionar las credenciales de autenticación a las entidades, ¿se identifican y registran éstos previamente de manera fidedigna ante el sistema, ante un Prestador Cualificado de Servicios de Confianza, o en un proveedor de identidad electrónica? *NOTA: Dicho proveedor ha de ser reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.*
	¿Se dispone de evidencias de que el usuario reconoce que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida?
N0	¿Se retiran y deshabilitan las credenciales cuando se detecta su pérdida o falta de control exclusivo por parte del usuario?
N0	¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que se autentica termina su relación con el sistema?
	¿La información suministrada en los accesos se restringe a la mínima imprescindible? NOTA: Se evita todo aquello que pueda revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo
N0	¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener éste el acceso?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

D.2.5: Gestión de derechos de acceso

El uso de los recursos del sistema se gestiona de forma que solo están disponibles para los usuarios autorizados.

Requisitos:

op.acc.2.1	- Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
op.acc.2.2	- Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
op.acc.2.r1.1	- Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.
op.acc.3	El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.
op.acc.3.1	- Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
op.acc.3.2	- Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.
op.acc.3.r1.1	Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema.
op.acc.3.r1.2	La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.
op.acc.3.r2.1	–Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.
op.acc.4	Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:
op.acc.4.1	– Todo acceso estará prohibido, salvo autorización expresa.
op.acc.4.2	– Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
op.acc.4.3	
op.acc.4.4	– Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
op.acc.4.5	–Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica. – Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Propuesta de evidencias:

	☐	Proceso de gestión de privilegios.
	☐	Evidencia de mecanismos de protección de los recursos (por ejemplo, documentación sobre roles, código que muestre la validación de los permisos antes de acceder al sistema, etc.)
	☐	Evidencia de asignación de responsables de los recursos.
	☐	Evidencia de criterios de acceso a los recursos (normativa, política, plantillas que determinen los privilegios a asignar en función del perfil, puesto, etc.)
	☐	Evidencia de auditorías de revisión de los permisos de acceso.
	☐	Evidencia de concesiones y revocaciones de accesos por el personal autorizado.
	☐	En su caso, la política de control de acceso.
	☐	En su caso, la política de acceso remoto.
	☐	Organigrama detallado de la organización que evidencie la segregación de funciones.
	☐	Evidencia de atributos de seguridad de los usuarios (individuales y de grupo).
	☐	Evidencia de granularidad de un usuario respecto a sus privilegios de acceso.
	☐	Evidencia de la existencia y control de cuentas con privilegios de auditoría y de que no tienen asignadas otras funciones

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Los recursos del sistema están protegidos con algún mecanismo que impida su utilización, salvo por las entidades que disfruten de derechos de acceso suficientes?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	**¿Los derechos de acceso de cada recurso, se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y/o normativa de seguridad del sistema?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se han determinado y se conocen las personas responsables de los diferentes recursos del sistema de información?
	¿Los derechos de acceso de cada recurso, se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y/o normativa de seguridad del sistema?
N0	¿Se han implementado los privilegios de acceso de modo que restrinjan con la suficiente granularidad el tipo de acceso que un usuario pueda tener (lectura, escritura, modificación, borrado, etc.)?
N0	**¿Se segregan aquellas funciones que, ante determinadas circunstancias, podrían culminar en conflicto de interés como, por ejemplo, desarrollo y operación?** ☐ SI ☐ NO
N0	¿Se evita, siempre que sea posible, que las capacidades de desarrollo y operación recaigan en la misma persona o en el mismo equipo? Nota: Cuando no sea posible, la organización deberá evidenciarlo.
N0	¿Se evita, siempre que sea posible, ¿que las personas que autorizan sean las mismas que controlan el uso? Nota: Cuando no sea posible, la organización deberá evidenciarlo.
	¿Se previenen más circunstancias de conflicto de interés, como puede ser, evitando concurran las ☐ SI ☐ NO
	¿Se evita, siempre que sea posible, que una misma persona aúne funciones de configuración y de mantenimiento del sistema? Nota: Cuando no sea posible, la organización deberá evidenciarlo.
	¿Quienes realizan funciones de auditoría o supervisión, no realizan ninguna otra función relacionada con lo auditado o supervisado? Nota: Esto afecta, en relación con las auditorías, especialmente al auditor interno, ya sea éste de la propia organización o contratado como prestación de servicios a una empresa externa.
N0	**¿Se gestionan los derechos de acceso, en base al principio de mínimo privilegio?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Está cualquier acceso prohibido, salvo que se disponga de autorización expresa?
	¿Se aplica una política de mínimo privilegio que reduce al mínimo imprescindible para cumplir con sus obligaciones los privilegios de cada entidad, usuario o proceso?
	¿Se asignan los privilegios de forma que las entidades, usuarios o procesos únicamente acceden al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones?
N0	¿Únicamente el personal con competencia para ello puede conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por el responsable de los mismos?
	¿Se ha establecido una política específica de acceso remoto, que señale la obligación de requerirse autorización expresa?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada' o N0*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*