Habilitaciones de seguridad para acceso a información clasificada o cargos sensibles

Experiencia de España y Estados Unidos de América

Autora

Bárbara Horzella Cutbill
Email: bhorzella@bcn.cl
Tel.: (56) 32 226 3160

Comisión

Elaborado para la Comisión de Control de Inteligencia del Estado de la Cámara de Diputados

Nº SUP: 155827

Resumen

El ingreso de personal a cargos que implican acceso a información clasificada o el desempeño de funciones sensibles está sujeto a procedimientos de habilitación de seguridad destinados a verificar la confiabilidad, integridad y lealtad institucional de los postulantes. La experiencia extranjera da cuenta de diversos mecanismos de control, previos al otorgamiento de una habilitación de seguridad, entre los que se cuentan: Verificación de identidad y antecedentes (administrativos, laborales, académicos y penales); Investigación patrimonial y financiera (análisis de deudas, patrimonio, conflicto de interés); Entrevistas personales (con postulante, colegas y superiores); Evaluaciones psicológicas; Exámenes médicos; Investigaciones del entorno (familiares, vínculos, etc.); así como revalidaciones periódicas ante eventuales cambios en la situación personal.

En términos generales, la experiencia española evidencia un sistema integral de protección de la información clasificada, que se materializa, entre otros aspectos, a través del proceso de Habilitación Personal de Seguridad, HPS, que a su vez se encuentra estrechamente vinculado a una estructura institucional especializada —encabezada por el Director del Centro Nacional de Inteligencia (CNI), quien como Autoridad Nacional para la Protección de la Información Clasificada (ANPIC) -a través de la Oficina Nacional de Seguridad (ONS)- establece criterios uniformes para toda la Administración del Estado y concentra las competencias para conceder, denegar, suspender o revocar las habilitaciones personales de seguridad.

EE.UU. en tanto, exhibe un modelo transversal de evaluación del personal (*personal vetting*) para toda la Administración Federal, donde priman los criterios de idoneidad (*suitability)* y aptitud (*fitness)* previo otorgamiento de una habilitación de seguridad (*security clearance*) para acceder a información clasificada, facultad que además presupone acreditar la necesidad de saber (*need-to-know*) y la suscripción de un acuerdo de confidencialidad (*non-disclosure agreement*). A diferencia del modelo español, en EE.UU. diversas instituciones están facultadas para emitir habilitaciones de seguridad. Sin embargo, autoridades como el Director de Inteligencia Nacional (*Director of National Intelligence, DNI*), que actúa como Agente Ejecutivo para la Seguridad (*Security Executive Agent, SecEA*), a través de la Dirección de Seguridad Especial (*Special Security Directorate, NCSC/SSD*) impulsan la coordinación y estandarización interagencial.

Introducción

A solicitud de la Comisión de Control de Inteligencia de la Cámara de Diputadas y Diputados, mediante Oficio N° 6/2026, el presente informe examina los mecanismos de habilitación de seguridad aplicables al ingreso de personal con acceso a información clasificada o al desempeño de cargos sensibles, a partir de la experiencia de España y Estados Unidos. Se describen los principales elementos institucionales, normativos y procedimentales de ambos sistemas, incluyendo las autoridades competentes, los procesos de investigación de antecedentes, los criterios de evaluación de idoneidad y las obligaciones posteriores al otorgamiento de la habilitación. Asimismo, se identifican las principales herramientas utilizadas para mitigar riesgos de seguridad derivados del personal, tales como investigaciones patrimoniales, evaluaciones psicológicas, controles periódicos y procesos de evaluación continua.

Para ello fue consultada la normativa nacional, así como sitios web oficiales.

El tema que se aborda y sus contenidos están delimitados por los parámetros de análisis acordados, por el plazo de entrega convenido y por la información disponible. No se trata de un documento académico y se enmarca en los criterios de neutralidad, pertinencia, síntesis y oportunidad en su entrega. Para el apoyo en las traducciones se utilizaron motores de IA.

I. España

En términos generales, la experiencia española evidencia un sistema integral de protección de la información clasificada, en el que las habilitaciones personales de seguridad constituyen solo uno de los componentes de una política más amplia de seguridad de la información. En este modelo, la evaluación de confiabilidad del personal se encuentra estrechamente vinculada a una estructura institucional especializada —encabezada por el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI), como Autoridad Nacional para la Protección de la Información Clasificada (ANPIC)— que establece criterios uniformes para toda la Administración del Estado y concentra las competencias para conceder, denegar, suspender o revocar las habilitaciones personales de seguridad.

1. Marco Normativo

La Ley 9/1968, sobre Secretos Oficiales, reconoce que, sin perjuicio del principio de publicidad que rige a la actuación de los órganos de Estado, existen ciertas materias que pueden ser declaradas expresamente como “clasificadas”, y su secreto o limitado conocimiento está amparado por ley (Artículo primero). A los efectos de esta ley, podrán ser declaradas como “materias clasificadas”, aquellos “asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado” (Artículo segundo).

En atención al grado de protección requerido, se establecen dos niveles de calificación, a saber: secreto y reservado (Artículo tercero), consagrando al Consejo de Ministros y a la Junta de Jefes de Estado Mayor, la facultad exclusiva e indelegable para calificar aquellas materias cuya difusión pueda poner en riesgo la seguridad o la defensa del Estado, respectivamente (Artículos cuarto y quinto).

Para efectos del tratamiento de la información clasificada, este régimen jurídico establece las siguientes disposiciones:

> A) Solamente podrán tener conocimiento de las «materias clasificadas» los órganos y las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen.
>
> B) La prohibición de acceso y las limitaciones de circulación a personas no autorizadas en locales, lugares o zonas en que radiquen las «materias clasificadas».
>
> C) El personal que sirva en la Administración del Estado y en las Fuerzas Armadas estará obligado a cumplir cuantas medidas se hallen previstas para proteger las «materias clasificadas». (Artículo octavo).

En este sentido, el Reglamento de la Ley 9/1968, contenido en el Decreto 242/1969, establece que los Servicios de Protección de Materias Clasificadas (SPIC) de los Departamentos ministeriales deberán asegurar el adecuado tratamiento de las materias sensibles; instruir al personal que tenga acceso a información clasificada respecto de las normas de protección; proteger aquel material clasificado bajo su custodia; así como mantener el registro de las materias clasificadas (Artículo noveno).

A mayor abundamiento, el artículo 33 del Reglamento "Programas de entrenamiento y ordenación" dispone lo siguiente:

> Las personas responsables de los Servicios de Protección de Materias Clasificadas establecerán y mantendrán programas activos de entrenamiento y orientación para loe *[sic]* funcionarios que en ellos presten sus servicios, a fin de inculcarles el sentido de la responsabilidad personal que, a cada uno, incumbe, en orden a proceder, en todo momento, con especial vigilancia y cuidado, al cumplimiento de las órdenes que reciba y a la más estricta observancia de las medidas de protección vigentes (…).

Por su parte, en las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, directrices que constituyen el desarrollo normativo por el que se regula el manejo de la información clasificada, esta última es clasificada como: "(…) cualquier información o material respecto del cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado una clasificación de seguridad". Y en función de su origen, se distingue entre:

> (…) información clasificada nacional (la que ha sido generada por los organismos del Estado y clasificada por los órganos con competencias para ello), e información clasificada internacional (la que ha sido generada por los organismos u organizaciones internacionales de los que España es país miembro, o por otros países con los que España ha concluido un acuerdo para la protección de información clasificada) (ONS, 2018:22).

A nivel nacional, a las clasificaciones consagradas en la ley de secretos oficiales, de "Secreto" y "Reservado", se suman aquellas materias de reserva interna, catalogadas como "Confidenciales" o de "Difusión limitada", que también requieren de protección (ONS, 2018:27).

2. Institucionalidad

Desde el punto de vista institucional y como se consigna en el reglamento aludido anteriormente, al interior de la administración pública española existen diversas reparticiones responsables de garantizar la protección de la información clasificada.

Con todo, el Secretario de Estado Director del Centro Nacional de Inteligencia (SEDCNI), dependiente del Ministerio de Defensa, constituye la Autoridad Nacional para la Protección de la Información Clasificada (en adelante, ANPIC)[1], responsabilidad que ejerce a través de la Oficina Nacional de Seguridad (ONS).

El tratamiento de la información clasificada es responsabilidad de los anteriormente mencionados Servicios de Protección de Información Clasificada (en adelante, SPIC), bajo el mando de un Jefe de Seguridad que rinde cuentas ante el jefe del organismo o entidad al que presta servicios, y que a su vez depende funcionalmente de la ANPIC, a través de la ONS.

Para su funcionamiento, los SPIC se organizan en unidades básicas denominadas órganos de control "que se extienden hasta los últimos escalones del ministerio, organismo o entidad en que se maneja la información clasificada" (ONS, 2018:34).

A mayor abundamiento:

> Los órganos de control son responsables de todos los aspectos relacionados con la seguridad de la información, es decir, tanto de su manejo y custodia (recepción, registro, almacenaje, distribución, etc.), como de la seguridad física, seguridad en el personal, seguridad en los sistemas de información y comunicaciones, etc. (ONS, 2018:34).

Para su funcionamiento se requiere personal con dedicación preferente, específicamente formado para ello, y con la autoridad suficiente; así como de medios e instalaciones de seguridad "específicamente adaptados y aprobados para la custodia, control y manejo de la información clasificada, constituidos como zona de acceso restringido (ZAR)" (ONS, 2018:35).

Por su parte, y aspirando a uniformar los procesos de protección de la información, la ANPIC ha emitido las siguientes normas (ONS, 2018:28):

- NS/00 para la protección de la información clasificada en España (principios básicos)
- NS/01 sobre estructura nacional para la protección de la información clasificada (requisitos orgánicos y funcionales)
- NS/02 sobre seguridad en el personal (Habilitación Personal de Seguridad, HPS)
- NS/03 sobre seguridad física (controles de acceso a la información)
- NS/04 sobre seguridad de la información (manejo de información clasificada)
- NS/05 sobre seguridad en los sistemas de información y comunicaciones

[1] La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, en su artículo 4, encomienda a este organismo la función de «Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada».

- NS/06 sobre seguridad industrial (contratos, proyectos o programas clasificados).

A continuación, se abordarán específicamente aquellas disposiciones respecto de las habilitaciones personales de seguridad.

3. Proceso de evaluación del personal

Según se establece en la norma NS/02, la Habilitación Personal de Seguridad (en adelante, HPS) constituye:

> (…) la resolución positiva de la ANPIC por la que, en nombre del Gobierno del Reino de España, reconoce formalmente a capacidad e idoneidad de una persona para tener acceso a información clasificada en el ámbito y grado autorizado, al haber superado el proceso de investigación de seguridad y haber sido concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento, resolución que se materializa en un documento firmado por la ANPIC (ONS, 2018:56).

En virtud de ello, la normativa española establece distintos grados, tipos y especialidades para la concesión de una HPS. Como "Grado" se define a la máxima clasificación de la información a la que se habilita el acceso (SECRETO (S), RESERVADO (R), CONFIDENCIAL (C)), en tanto que el "Tipo", corresponde al origen de la información, es decir, organización (OTAN, UE o ESA) o país, por ejemplo. Por último, la "Especialidad" se refiere a aquellos ámbitos que exigen una especial preparación del usuario y un control más exhaustivo (por ejemplo, ATOMAL, CRYPTO o BOHEMIA en el ámbito internacional o CRIPTO y SIGINT, en el nacional).

Concretamente, la investigación de seguridad constituye un análisis de riesgos realizado sobre la persona y su entorno, con el objeto de identificar y valorar las vulnerabilidades y amenazas que se ciernen sobre el interesado, y con ello determinar un grado de riesgo que resulte aceptable para España. Con ese fin, la ANPIC establece un listado de criterios a ser relevados durante las investigaciones (véase Anexo).

Desde el punto de vista institucional, la NS/01 establece que la ANPIC es responsable de: "Valorar la idoneidad de las personas que deban tener acceso a la información clasificada y emitir el correspondiente certificado en forma de Habilitación Personal de Seguridad (HPS)", ostentando la competencia exclusiva para conceder, denegar, suspender o retirar las HPS. (ONS, 2018:31).

A su vez, la ONS, como órgano de trabajo de la ANPIC es responsable de la gestión y control de los procesos para determinar dicha idoneidad, pudiendo solicitar cuanta información adicional precise.

Existen organismos que cuentan con capacidades de investigación propias para determinar las condiciones de seguridad de su personal. Tal es el caso de los tres Ejércitos, las Fuerzas y Cuerpos de Seguridad Estado y del CNI (ONS, 2018:71). En caso de necesidad, la ONS puede realizar investigaciones complementarias.

En este sentido, los órganos de control de los SPIC, son los encargados de “Centralizar la tramitación de los expedientes de solicitud de habilitación personal de seguridad correspondientes a sus organismos dependientes, y apoyar en las investigaciones cuando así les sea requerido por la ONS” (ONS, 2018:39).

Todas aquellas personas que manejen información clasificada de grado “CONFIDENCIAL o equivalente” o superior, los encargados de su custodia y traslado, y, en general, cualquiera que pudiera contar con la posibilidad razonable de tener acceso a ella, deberán disponer de una HPS.

Con todo, el acceso a información clasificada solo podrá materializarse previa verificación de los siguientes requisitos: estar en posesión de una HPS; recibir la instrucción de seguridad preceptiva; y demostrar la “necesidad de conocer” (ONS, 2018:57).

Desde el ámbito procedimental, la tramitación de una HPS implica que:

> El interesado conoce, y autoriza, que va a ser sometido a un proceso de investigación sobre su persona y su entorno. La investigación será más exhaustiva en función del grado de información clasificada al que se necesite acceder. Para ello el interesado debe aportar al expediente de solicitud los datos iniciales para su realización. Durante el transcurso de la investigación se le podrán solicitar los datos adicionales que se estimen necesarios para determinar el riesgo (ONS, 2018:62).

Además, durante la vigencia de la HPS, el interesado estará sometido a un proceso de evaluación continua de seguridad, debiendo además comunicar cambios significativos en su situación personal desde el momento de la concesión de la HPS.

El periodo de tramitación de una HPS no debería exceder los seis meses, a menos que se requieran antecedentes adicionales. Las HPS se conceden inicialmente por un periodo de cinco años -salvo aquellas otorgadas con carácter restringido- y definen explícitamente el tipo de información clasificada al que se confiere acceso (grado, tipo y especialidades), así como su fecha de caducidad.

4. Práctica

Para acceder a trabajar al CNI, se establecen los siguientes requisitos generales de ingreso (CNI, 2026):

1. Tener nacionalidad española.
2. Estar en posición de un título académico acorde a grupo o subgrupo que se opte.
3. No haber sido separado mediante expediente de ninguna de las Administraciones Públicas, ni hallarse inhabilitado para el ejercicio de funciones públicas, ni privado del ejercicio de derechos civiles.
4. Ser mayor de edad.
5. No padecer enfermedad o defecto físico que incapacite para el ejercicio de las funciones del puesto.
6. Poseer o estar en condiciones de obtener el informe favorable de seguridad acorde a las características propias del puesto de trabajo que vaya a ocupar.

Al respecto, y según se consigna en el Estatuto del Personal del CNI (Real Decreto 240/2013):

> Para asegurar la objetividad y racionalidad del proceso selectivo, éste estará constituido por un conjunto de pruebas cuyo contenido se adecuará al desempeño de las tareas de los puestos de trabajo convocados. Sin perjuicio de las excepciones que pudieran establecerse en función de la especialidad del puesto de trabajo convocado, el proceso de selección incluirá la valoración de méritos de los aspirantes, la realización de pruebas psicotécnicas y de personalidad, la comprobación de los conocimientos y capacidades de los aspirantes, expresados de forma oral, escrita y, en su caso, a través de pruebas prácticas, así como la comprobación del dominio de lengua extranjera.
>
> En aquellos puestos de trabajo para los que se exija un nivel determinado de condiciones físicas, se podrá exigir la superación de las pruebas que reglamentariamente se determinen.
>
> El proceso se completará con cuantas entrevistas personales fuesen necesarias a juicio del órgano de selección para asegurar la adecuación del candidato al puesto de trabajo convocado (art.11, núm.2)

De forma preliminar, la ONS lleva a cabo los denominados informes de seguridad, cuyo contenido es definido por el Secretario General del CNI a través de normativa interna. Los antecedentes personales de los postulantes son evaluados, para determinar si estos reúnen las condiciones mínimas de confiabilidad para ser incorporados al servicio. Únicamente aquellos aspirantes con un informe favorable son incluidos en la base de datos de candidatos que continuarán el proceso de selección.

La selección de los aspirantes, a partir de sus resultados en los distintos procesos de avaluación es realizada por un tribunal de selección, órgano colegiado y especializado del CNI (art.10), cuya propuesta, junto con los respectivos antecedentes, es elevada al Secretario General, quien la remite a su vez al Secretario de Estado Director del CNI para el nombramiento del personal, ya sea como estatutario temporal o en prácticas[2].

Para adquirir la condición de personal estatutario temporal, los aspirantes deben cumplir los siguientes requisitos (art.12):

a) Superación del proceso selectivo.
b) Nombramiento por el Secretario de Estado Director.
c) Acatamiento de la Constitución como norma fundamental del Estado y de este Estatuto.
d) Toma de posesión del puesto de trabajo.
e) Aceptación del compromiso de permanencia.

A través de este último, el personal se compromete "(…) a prestar servicios por un plazo mínimo de cuatro años, contados desde la fecha de toma de posesión del puesto de trabajo, sin perjuicio de la facultad del CNI de cesar al personal antes del transcurso de dicho plazo". Con todo, estos funcionarios estarán sujetos "(…) a un periodo de valoración de idoneidad que comprenderá los procesos de

[2] En determinados puestos se solicita como requisito adicional la aprobación de un curso de formación, período en que el aspirante tiene la condición de personal estatutario en prácticas. De no superar el curso, no se adquiere la condición definitiva.

formación y los periodos de prueba adecuados para la valoración del correcto desempeño del correspondiente puesto de trabajo", cuya duración no podrá exceder de dos años.

A partir de los cinco años en funciones, y previa evaluación del Secretario General, se ofrece al personal temporal la posibilidad de integrarse de forma permanente al servicio. Quienes declinen el ofrecimiento cesarán en el CNI en un plazo máximo de seis meses contados desde el ofrecimiento, en tanto quienes acepten, deberán firman un nuevo compromiso de permanencia por un plazo mínimo de cinco años (art.13).

El Estatuto, aborda el "Historial profesional" (art.15) donde se regulan los datos y antecedentes que deben constar en: a) el Expediente personal (art.16), b) Informes personales (art.17), c) Expediente académico (art.18), y d) Expediente de aptitud psicofísica (art.19), a su vez, el artículo 20 está consagrado a las "Evaluaciones" del personal, señalando que estas permiten:

a) Valorar su idoneidad como personal temporal.
b) Valorar su competencia y cualificación para adquirir la condición de personal estatutario permanente.
c) Valorar su competencia y rendimiento en el desempeño de su puesto de trabajo.
d) Valorar sus competencias, experiencia y trayectoria profesional para la evaluación en los distintos sistemas de carrera profesional.
e) Determinar los posibles riesgos personales de seguridad para el CNI.
f) Participar en las modalidades de formación profesional.
g) Determinar la existencia de insuficiencia de facultades profesionales o de condiciones psicofísicas.

Por su parte, el Capítulo V "Deberes del personal estatutario" consagra la obligación del personal de contribuir con las investigaciones de seguridad que le afecten (art.74), así como el deber de guardar el secreto "sobre las actividades del CNI, su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información (…)", entre otras materias de carácter clasificado y no clasificado (art.75).

Asimismo, el CNI podrá exigir los siguientes antecedentes a sus funcionarios (art. 77):

a) Las declaraciones tributarias correspondientes al Impuesto sobre la Renta de las Personas Físicas y al Impuesto Extraordinario sobre el Patrimonio.
b) Los bienes y derechos patrimoniales que posea.
c) Los valores o activos financieros negociables.
d) Las participaciones societarias.
e) El objeto social de las sociedades de cualquier clase en las que tenga intereses.

II. Estados Unidos de América (EE.UU.)

A nivel federal, el Gobierno de los Estados Unidos de América (en adelante, EE.UU.) ha implementado un proceso integral de investigación y evaluación continua del personal (*Personell Vetting Process)*, con el objeto de determinar su idoneidad (*suitability*) y aptitud (*fitness*) para el desempeño de determinados cargos o responsabilidades, en el marco de la política conocida como "*Trusted Workforce 2.0*".

1. Marco normativo

La normativa estadounidense, a través de la Orden Ejecutiva 12958 (*Executive Order, EO 12958*), establece un sistema común a toda la Administración Federal para la clasificación, custodia y desclasificación de información en materia de seguridad nacional, distinguiéndose tres niveles de acceso a información clasificada (*Confidential, Secret y Top Secret*).

En este sentido, la Orden Ejecutiva 12968 (*EO 12968*), determina que únicamente se puede acceder a información clasificada si se cumplen las siguientes condiciones: obtener una "habilitación de seguridad" (*security clearance*), demostrar la necesidad de acceso a dicha información *(need-to-know*), y haber suscrito el acuerdo de confidencialidad (*non-disclosure agreement*), donde se consigna la responsabilidad de proteger la información y posibles consecuencias de una divulgación no autorizada (*unauthorized disclousure*).

En particular, las habilitaciones de seguridad (*security clearance*), entendidas como autorizaciones para acceder a información clasificada, operan tanto para el ingreso de personal a una entidad o cargo determinado, la reevaluación periódica del personal en funciones; el acceso a información clasificada, así como para el compartimentaje de información sensible entre diversas reparticiones. En particular, la Orden Ejecutiva 13467 (*EO 13467*) consagra el concepto de "*adjudication*" como:

> (…) la evaluación de datos pertinentes obtenidos en una "Investigación de Antecedentes" (*Background Investigation*), así como de cualquier otra información disponible que sea relevante y confiable, para determinar si un individuo:
>
> i) es idóneo para desempeñarse en un empleo público;
>
> ii) reúne los requisitos para obtener acceso lógico y físico a sistemas e instalaciones;
>
> iii) es elegible para acceder a información clasificada;
>
> iv) es apto para ocupar un cargo sensible; o
>
> v) es idóneo para desempeñar funciones para el Gobierno o en su representación, como contratista.

La norma aplica a todos aquellos individuos (*covered individual*) que desempeñen o pretendan desempeñar funciones para el Poder Ejecutivo o en su representación, excluyendo expresamente al Presidente de los EE.UU., al Vicepresidente, y sus funcionarios directos, salvo instrucción en contrario.

2. Institucionalidad

Diversas reparticiones gubernamentales de los EE.UU. están facultadas para emitir habilitaciones de seguridad, previo proceso de verificación de requisitos y valoración de antecedentes del postulante (*personnel vetting)*.

En ese contexto, la *EO 13467*, anteriormente aludida, promueve la utilización de procedimientos y criterios estándares, así como innovaciones tecnológicas que permitan un intercambio fluido de información entre las distintas reparticiones federales. De esta forma, y salvo que la ley disponga otra cosa, las investigaciones de antecedentes y los procesos de adjudicación deben ser reconocidos y aceptados mutuamente y de manera recíproca por todos los organismos.

Por su parte, y a efectos de una mayor coordinación y estandarización interagencial, la misma Orden dispuso el establecimiento de un Agente Ejecutivo para la Idoneidad (*Suitability Executive Agent*), como autoridad designada para dirigir y coordinar las políticas federales relativas a la evaluación de la idoneidad de las personas para desempeñar empleos públicos, facultad actualmente radicada en la Oficina de Gestión de Personal (*U.S. Office of Personnel Management, OPM, 2026*); así como de un Agente Ejecutivo para la Seguridad (*Security Executive Agent, SecEA*), encargado de implementar y supervisar las políticas y procedimientos relativos a las habilitaciones de seguridad para el acceso a información clasificada y la ocupación de cargos sensibles, responsabilidad que recae en el Director de Inteligencia Nacional (*Director of National Intelligence, DNI*) para lo que cuenta con la Dirección de Seguridad Especial (*Special Security Directorate, NCSC/SSD*) como órgano ejecutivo.

Ambos Agentes Ejecutivos responden al Consejo de Rendición de Cuentas sobre el Desempeño en Materia de Idoneidad y Habilitaciones de Seguridad (*Suitability and Security Clearance Performance Accountability Council*, PAC), que a su vez es responsable ante el Presidente de los EE.UU. (DNI,2026).

3. Proceso de evaluación de personal

En términos prácticos, el proceso de evaluación de personal (*Personell Vetting Process*) inicia cuando el postulante a un empleo recibe una oferta de trabajo condicionada y es contactado por un Coordinador de Habilitaciones de Seguridad (*Clearance Coordinator*), quien lo asiste en la presentación de los formularios y documentos requeridos (*Department of State*, 2026).

Una vez entregada la información, la agencia interesada inicia formalmente la Investigación de Antecedentes (*Background Investigation*), proceso en que las huellas dactilares y registros personales son contrastados con bases de datos comerciales y gubernamentales, y antecedentes biográficos relevantes son verificados mediante entrevistas a contactos.

Finalizada la investigación, se determina la idoneidad del postulante, para ser merecedor de una habilitación de seguridad nacional, ya sea para acceder a información clasificada o a un puesto sensible, o bien para que le sea otorgada una credencial federal para acceder a sistemas o instalaciones.

El postulante es notificado de la decisión final a través de la agencia contratante. En caso de un resultado desfavorable, el postulante puede retirarse del proceso o bien apelar la decisión.

Además, en casos excepcionales el sistema permite que, una vez iniciada la investigación de antecedentes, se adopte una “determinación preliminar o interina” (*preliminary or interim determination*), que permite al postulante iniciar sus funciones antes de la conclusión del proceso de evaluación.

4. Práctica

En el *Federal Bureau of Investigation* (en adelante, FBI), para ser elegible a un cargo se deben cumplir los siguientes requisitos generales (FBI, 2026):

- Ser ciudadano de los Estados Unidos (*U.S. citizen*)
- Mantener antecedentes públicos en regla y no haber sido condenado por un delito grave (*felony*).
- Cumplir con la política del FBI sobre consumo de drogas.
- Aprobar un examen de orina para detección de drogas y la investigación de antecedentes (*Background investigation*).
- Mantener al día el pago de préstamos estudiantiles.
- Haber presentado todas las declaraciones tributarias federales, estatales y locales exigidas.
- Encontrarse al día en el pago de las obligaciones de manutención de hijos establecidas judicialmente.
- No haber participado en organizaciones destinadas a derrocar al Gobierno de los Estados Unidos.
- Haberse registrado en el Sistema de Servicio Selectivo (*Selective Service System*), en el caso de los postulantes hombres, con las excepciones establecidas por la normativa.

Para desempeñarse como agente especial (*Special Agent*), además de cumplir los requisitos generales de elegibilidad para trabajar en el FBI, los postulantes deben satisfacer los siguientes requisitos específicos (FBI, 2026a):

- **Nivel GL-9[3]:** poseer un título universitario de pregrado y un año de experiencia como funcionario de seguridad pública con facultades de policía (*sworn law enforcement officer*), o bien poseer un título de posgrado.
- **Nivel GL-10:** poseer un título universitario de pregrado y, al menos, dos años de experiencia laboral profesional a tiempo completo, o bien un título de posgrado y, al menos, un año de experiencia laboral profesional a tiempo completo.
- Tener al menos 23 años de edad.
- Presentar la postulación antes de cumplir 36 años, salvo las excepciones aplicables a personas con preferencia por su condición de veteranos o con experiencia previa en organismos federales encargados de hacer cumplir la ley. En todo caso, el postulante debe completar el proceso de selección (*Special Agent Selection System*, SASS) e ingresar al servicio, a más tardar, el día anterior a cumplir 37 años.
- Poseer una licencia de conducir válida.
- Cumplir los requisitos físicos establecidos por el FBI y aprobar la prueba de aptitud física correspondiente.
- Cumplir los requisitos médicos exigidos para el cargo.
- Encontrarse legalmente habilitado para poseer y portar armas de fuego.

[3] Estos niveles corresponden a grados salariales de clasificación en el Sistema Federal.

- Ser elegible para obtener una habilitación de seguridad Top Secret (*FBI Top Secret security clearance*) con acceso a información compartimentada sensible (*Sensitive Compartmented Information, SCI*).

Respecto a este último punto, la investigación de antecedentes (*Background Investigation*) incluye una prueba de polígrafo.

Al respecto, se indica:

> Los requisitos preliminares para el empleo comprenden un examen poligráfico; una prueba de detección del consumo de drogas ilícitas; verificaciones de solvencia económica y de antecedentes; así como entrevistas exhaustivas con antiguos y actuales colegas, vecinos, amigos, profesores, entre otros. Antes de presentar una solicitud para cualquier cargo en el FBI, asegúrese de que las causales de inhabilitación laboral establecidas por dicha institución no le resulten aplicables (FBI, 2026b).

Anexo

Criterios de valoración de idoneidad de las personas (Normas ANPIC)

a) La participación, conspiración, ayuda o inducción a la comisión de actos de sabotaje, espionaje, terrorismo, traición o sedición,
b) La colaboración o relación, de forma interesada o inconsciente, con un servicio de inteligencia o gobierno extranjero que pueda constituir una amenaza para la seguridad de España, de la OTAN, de la Unión Europea o de sus Estados Miembros o de otros aliados del Reino de España. Quedan excluidas las relaciones autorizadas de carácter oficial.
c) La asociación, adscripción, afinidad ideológica, amistad o complicidad con organizaciones, grupos o personas que utilicen medios violentos o ilícitos para subvertir el orden constitucional de España o de sus aliados.
d) La pertenencia o afinidad del interesado a asociaciones, grupos o fundaciones, cualesquiera que sea su forma jurídica, que pudiera suponer un conflicto de lealtades con la protección de la información clasificada.
e) La falta de acatamiento a la Constitución y al ordenamiento jurídico de España o de la Unión Europea.
f) La asociación, adscripción, afinidad, amistad o complicidad con organizaciones, grupos o personas, cuyas actividades impidan a otros el ejercicio de sus libertades y derechos constitucionales.
g) La falta de colaboración o el intento de engaño en la investigación de seguridad.
h) Falsear, ocultar, mentir, o no aportar la información o los datos requeridos, durante el proceso de tramitación de la solicitud de HPS o durante la vigencia de la misma.
i) La existencia de deudas con la Administración tributaria o la seguridad social de España o de otros Estados Miembros de la Unión Europea, derivadas de engaño o fraude.
j) La detección de indicios de actividades delictivas, independientemente de que deriven o no en responsabilidades penales.

k) La existencia de dificultades financieras graves.
l) La existencia de ingresos patrimoniales injustificados.
ll) El consumo reiterado de drogas ilegales o el consumo abusivo de drogas lícitas.
m) El abuso en el consumo de bebidas alcohólicas.
n) Cualquier adicción, dependencia o conducta, pasada o actual, reiterada e incontrolada, que pueda afectar de forma significativa a las normas de convivencia o suponer una vulnerabilidad personal por chantaje o presión.
o) La falta de discreción relativa a su vida privada o laboral que pueda derivar en una vulnerabilidad personal.
p) La falta de fiabilidad.
q) La falta de honradez.
r) La falta de lealtad.
s) Haber infringido reiteradamente las normas de seguridad establecidas o haber causado un daño grave a la organización por su incumplimiento.
t) El acceso no autorizado a sistemas informáticos o de telecomunicaciones, tanto en su vida profesional como en la privada, vulnerando las medidas de seguridad y la normativa de utilización de estos.
u) La realización de actividades reiteradas en beneficio propio, en perjuicio grave de terceros
v) La existencia de informes laborales que evidencien conductas conflictivas o acciones reivindicativas llevadas a cabo por medios ilegales.
w) La existencia de informes médicos que evidencien que el interesado padece una psicopatología con afectación al juicio de realidad o a la responsabilidad de sus actos.
x) La existencia de evidencias de grado inasumible de estulticia que pueda derivar en una vulnerabilidad personal.
y) La existencia de cualesquiera aspectos que pudieran ser utilizados como medio de coacción para obtener información.
z) Cualquier otra circunstancia que específicamente no esté contemplada en los criterios anteriores y que pueda suponer una vulnerabilidad.

Referencias

CNI (2026) Trabaja con nosotros. Disponible en: https://www.cni.es/trabaja-con-nosotros/trabaja-en-el-cni (septiembre, 2026).

Department of State (2026) Security Clearances. Disponible en: https://www.state.gov/securityclearances (septiembre, 2026).

FBI (2026) *Eligibility and Hiring. What it takes to join the FBI*. Disponible en: https://fbijobs.gov/eligibility (septiembre, 2026).

FBI (2026a) *Special Agent Eligibility*. Disponible en: https://fbijobs.gov/special-agents/application-and-evaluation-process#eligibility (septiembre, 2026).

FBI (2026b) *Employment Eligibility*. Disponible en: https://fbijobs.gov/sites/default/files/2025-02/guide_eligibility.pdf (septiembre, 2026, 2026).

DNI (2026) *Security Executive Agent*. Disponible en: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent (septiembre, 2026, 2026).

OPM (2026) *Suitability Executive Agent.* Disponible en: https://www.opm.gov/suitability/suitability-executive-agent/ (septiembre, 2026, 2026).

Referencias normativas

España

Ley 9/1968, de 5 de abril, sobre secretos oficiales. Disponible en: https://www.boe.es/eli/es/l/1968/04/05/9/con (septiembre, 2026).

Ley 11/2002, de 6 de mayo de, reguladora del Centro Nacional de Inteligencia. Disponible en: https://www.boe.es/eli/es/l/2002/05/06/11/con (septiembre, 2026).

Real Decreto 240/2013, de 5 de abril de, por el que se aprueba el Estatuto del personal del Centro Nacional de Inteligencia. Disponible en: https://www.boe.es/eli/es/rd/2013/04/05/240 (septiembre, 2026).

ONS (2018) Normas de la Autoridad Nacional para la Protección de la Información Clasificada. Disponible en: https://sede.defensa.gob.es/acceda/tablon/descargarfichero?id=952 (septiembre, 2026).

EE.UU.

Executive Order 12958, *Classified National Security Information*, de 17 de abril de 1995. Disponible en: https://www.govinfo.gov/content/pkg/WCPD-1995-04-24/pdf/WCPD-1995-04-24-Pg634.pdf (septiembre, 2026).

Executive Order 12968, Access to Classified Information, de 2 de Agosto de 1995. Disponible en: https://www.govinfo.gov/content/pkg/WCPD-1995-08-07/pdf/WCPD-1995-08-07-Pg1365.pdf (septiembre, 2026).

Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, de 30 de junio de 2008. Disponible en: https://www.govinfo.gov/content/pkg/WCPD-2008-07-07/pdf/WCPD-2008-07-07-Pg932.pdf (septiembre, 2026).

Nota aclaratoria

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.

Creative Commons Atribución 3.0
(CC BY 3.0 CL)