Estudio sobre la amenaza interna en el ámbito de las Infraestructuras Críticas

FUNDACIÓN BORREDÁ
al servicio de la seguridad

PREÁMBULO

La cuestión de los *"insiders"*, que más correctamente podríamos denominar **amenaza interna**, es un asunto que viene preocupando en el Ministerio del Interior, especialmente en el ámbito de las infraestructuras críticas, hasta el punto de que el CNPIC trabaja desde hace tiempo en dotar a los operadores críticos de instrumentos para hacer frente a esta amenaza.

En esta línea, una vez más el CNPIC ha confiado en la fiabilidad y objetividad de la Fundación Borredá y en su amplio conocimiento del mundo de la seguridad, para colaborar en la búsqueda de fórmulas que permitan el mejor tratamiento del problema. Yendo aún más allá, el Centro ha servido de puente entre la Fundación y los operadores críticos, generando las sinergias necesarias para facilitar un estudio riguroso.

Como ejemplo de esta colaboración, 60 Responsables de Seguridad y Enlace de otros tantos operadores contestaron al cuestionario que les fue remitido y pudimos establecer, con conocimiento de causa, la situación real de la lucha contra la amenaza interna en el entorno de las infraestructuras críticas. Apoyándonos en este conocimiento, hemos incorporado al estudio algunas consideraciones jurídicas y de orden práctico, que nos permiten formular interesantes conclusiones y recomendaciones para orientar la acción de las Autoridades.

Queda, pues, patente el interés del CNPIC por enfrentarse al problema y emprender acciones reales para minimizar los riesgos. Cumpliendo su función impulsora del Sistema, ha dinamizado la participación de los operadores, pero sería injusto no señalar aquí la proactividad de éstos, que se han implicado formidablemente en ofrecernos un retrato veraz de la situación y abrir nuestros ojos a problemas que no siempre son correctamente percibidos desde el exterior.

Es el momento de expresar nuestro especial agradecimiento al CNPIC y a los operadores críticos por su confianza en la Fundación Borredá. Nuestro compromiso con la seguridad queda cumplido con la elaboración de este informe y la consiguiente aportación a la Administración de elementos de juicio para valorar correctamente la situación, abriendo vías de actuación para que pueda combatir eficazmente la amenaza. En sus manos queda ahora elegir los instrumentos más adecuados a este propósito.

ÍNDICE

1. INTRODUCCIÓN

1.1 La responsabilidad de la protección de las infraestructuras críticas

En un mundo de amenazas globalizadas, la provisión de los servicios esenciales que constituyen el soporte de nuestros Estados del Bienestar, se encuentra en el punto de mira de cualquier clase de organización criminal, tanto si se trata de delincuencia organizada, como de grupos terroristas, o incluso de organizaciones gubernamentales y grupos de presión, que conociendo los devastadores efectos que, en términos de impacto social, tiene la interrupción de estos servicios para la estabilidad de un país, toman como potencial objetivo permanente de sus ataques las infraestructuras de todo tipo que les dan soporte.

Conscientes de esta realidad, tanto los propios Estados como las organizaciones supranacionales vienen tomando medidas encaminadas a mejorar la protección de estas infraestructuras, teniendo en cuenta que, siendo la interdependencia una de sus características más notorias, resulta de primordial importancia fijar unos estándares comunes elevados para mejorar su protección, en la inteligencia de que la fortaleza del sistema se mide por la de su eslabón más débil.

Así, en el ámbito de la Unión Europea, la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, vino a culminar un proceso de normalización iniciado a raíz de los atentados de Madrid en 2004, en el que, a través de diversas Comunicaciones, se instaba a los Estados miembros a mejorar la protección de sus infraestructuras críticas. Como elemento fundamental, esta Directiva consagra explícitamente el principio de que la responsabilidad principal y última de su protección corresponde a los Estados y a los propietarios u operadores de tales infraestructuras. Por su parte, España transpuso esta norma a su propio ordenamiento jurídico a través de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, desarrollada a su vez por toda una batería de normas de segundo y tercer nivel que configuran un sistema de protección sólido, que va perfeccionándose progresivamente para evitar espacios de inseguridad.

Más adelante, tomando conciencia de que las redes y sistemas de información desempeñan un papel crucial en la sociedad, hasta el punto de que su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior, se promulga la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esta norma se transpone a nuestro ordenamiento mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. En él se imponen tanto a operadores de servicios esenciales como a proveedores de servicios digitales, una serie de obligaciones referidas a su seguridad y a la notificación de incidentes, que habrán de concretarse, en muchos casos, mediante las correspondientes normas de segundo y tercer nivel.

En definitiva, tanto las Autoridades de la UE como las españolas vienen realizando un esfuerzo, tan importante como necesario, para dotar a nuestros servicios esenciales y a las infraestructuras que les dan soporte de un sistema de protección eficaz en el que Estado y operadores comparten la responsabilidad de garantizar su protección. En este sentido, estando concebido este sistema como algo dinámico y sometido a constante evolución y mejora para evitar la aparición de espacios de debilidad que mermen la fortaleza del conjunto, conviene llamar la atención sobre la existencia de uno de estos espacios, cual es el de la amenaza interna, en el que, por falta de previsión de las autoridades reguladoras, se abre una vía a la intervención de elementos terroristas o simplemente desestabilizadores.

1.2. La amenaza interna

Este sistema de protección de las infraestructuras críticas, basado en la planificación, tiene uno de sus pilares en el análisis de riesgos incorporado a los planes de protección como un elemento de sistematización de los riesgos a los que está sometida una determinada instalación u operador, frente a los que han de oponerse las medidas de seguridad más adecuadas para su minimización. En este sentido, cada operador debe analizar su propia situación y valorar adecuadamente las posibles vías de materialización de sus amenazas, entre las que siempre deberá tener en cuenta las que proceden del interior de su propia organización o, incluso, de debilidades del sistema.

En la Fundación Borredá consideramos que la amenaza conocida como interna, en el ámbito de las infraestructuras críticas, **procede básicamente de los empleados propios o del personal externo al servicio de compañías proveedoras**, actual o pasado, que movidos por diferentes motivaciones producen, o colaboran con terceros, en la producción deliberada de daños a la organización. En función del acceso que tengan permitido a áreas o informaciones sensibles del operador, parece necesario certificar su probidad, antes de la contratación y durante su permanencia en la empresa, en base a comprobaciones de sus antecedentes penales y de conducta.

Ciertamente hay que contemplar también como una forma de amenaza interna la posibilidad de que se produzcan daños internos o a terceros como consecuencia de la **incompetencia o negligencia** de empleados propios, o de proveedores, con acceso a áreas sensibles; o por la **mala praxis** de personas con privilegios de acceso en la organización que violan los protocolos de seguridad establecidos. Frente a estos casos, en los que no existe a priori intencionalidad de causar daño, debe oponerse un **plan de formación** adecuado para concienciar a todo el personal en la necesidad de prestar la debida atención en su desempeño profesional, con los filtros necesarios para garantizar una adecuada aptitud técnica. En este informe se propondrán algunas medidas, a modo de **buenas prácticas**, para anticiparse al problema y dotarse de las capacidades necesarias para minimizar sus efectos.

Por otra parte, existe un elemento potenciador de cualquier amenaza, incluidas las internas, al que podríamos denominar **incongruencia normativa**, en virtud de la cual el cumplimiento de determinadas normas, o la falta de otras, colisiona con los objetivos de protección exigidos por la normativa PIC. Esta disfunción es lamentablemente frecuente en la realidad y procede del propio sistema, porque es el legislador quien pierde el sentido de la prioridad en los bienes jurídicos a proteger. Obviamente, su corrección está sólo en manos de las autoridades reguladoras, que deben actuar convenientemente dirigidas en una acción coordinada hacia un objetivo común, porque de nada sirven los esfuerzos de los operadores para minimizar riesgos si otras normas que también les afectan desvirtúan sus dispositivos de seguridad. En este sentido, el informe incluye una recomendación para corregir por Ley esta situación.

Centrándonos en los empleados propios y de terceros que actúan maliciosamente, la probabilidad de ocurrencia es más que previsible, especialmente en determinados ámbitos. Pero si bien es cierto que corresponde a los propios operadores adoptar las medidas de seguridad necesarias para la minimización del riesgo, no lo es menos que debe producirse una convergencia entre la acción pública y privada mediante normas que regulen el intercambio de la información necesaria para llevar a cabo comprobaciones de idoneidad y probidad sobre el personal y den soporte jurídico a las acciones que los operadores deban tomar como consecuencia de la aparición de circunstancias que puedan considerarse como amenaza.

En consecuencia, este informe tiene por objeto proponer y justificar una serie de medidas legales y organizativas dirigidas a prevenir el riesgo de que elementos malintencionados con acceso a áreas o informaciones sensibles de operadores o infraestructuras críticas, estén dispuestos a actuar por sí mismos o a colaborar con otros, bajo cualquier motivación, en la producción de daños a las personas o a los activos de la empresa, o a la población.

El fenómeno es conocido, toda vez que existen datos de acciones terroristas perpetradas con apoyo de colaboradores en el interior de las organizaciones para atentar contra ellas. En este sentido, la Declaración del Contexto Mundial de Riesgo para la seguridad de la aviación de la Organización de Aviación Civil Internacional (ICAO Global Risk Context Statement), confirma que las organizaciones terroristas siguen considerando que los elementos internos, dependiendo de su función, son un recurso potencialmente útil para facilitar la planificación de ataques, ya sea de manera deliberada o no deliberada, por voluntad propia o bajo coerción, debido a su conocimiento especializado de las medidas de seguridad y su posible acceso a las zonas de seguridad restringidas y a las aeronaves.

En nuestro terrorismo autóctono más reciente, es sabido que ETA, al margen de otras acciones en esta línea, utilizaba informaciones facilitadas por empleados afines a la banda para extorsionar o atentar contra los propietarios de las empresas donde trabajaban. Por lo que se refiere a yihadismo, podemos citar algunos hechos relevantes relacionados con este tipo de amenaza:

- Lyon, Francia, 26 de julio de 2015. Un individuo entró con su furgoneta en la empresa americana Air Products, situada en el polígono industrial de Saint-Quentin-Fallavier, en el departamento de Isère, cerca de Lyon. Trabajador en la empresa, le abrieron la puerta y seguidamente, tras precipitar el vehículo contra un hangar abierto con bombonas de gas, se produjo una explosión que hirió a dos empleados. Previamente, el individuo había asesinado y decapitado a un directivo de la empresa, cuya cabeza colgó de una verja en el interior.

- Península del Sinaí, 31 de octubre de 2015. Atentado en vuelo contra avión ruso Airbus –321, con origen Egipto y destino San Pestesburgo, reivindicado por DAESH. Murieron 224 personas. Aparentemente, cometido con un pequeño artefacto colocado en una lata de refresco bajo los asientos del pasaje. Existen fundadas sospechas de que pudo haber sido introducido por algún trabajador perteneciente al personal de tierra del aeropuerto de partida.

- Kabul, 11 de noviembre de 2015. Atentado contra embajada española, ocasionando 10 muertos (2 miembros de CNP). Se sospecha que el comando disponía de información precisa del interior de la embajada y que pudo ser facilitada por algún trabajador de la misma.

- Diciembre de 2018. En el ámbito de la ciberseguridad, informaciones periodísticas dan cuenta de un ciberataque selectivo, dirigido exclusivamente a una serie de ordenadores de altos directivos de una empresa española del sector de la energía. Un técnico, perteneciente a un proveedor externo de servicios, robó algunas contraseñas particulares de ejecutivos y amenazó a la compañía con difundir la información a la que había tenido acceso sobre documentos altamente confidenciales, operaciones de fusiones y adquisiciones y objetivos estratégicos potenciales de la corporación.

1.3. Algunos tipos de respuesta

El ejemplo más elocuente de actuación permanente de los reguladores para combatir la amenaza interna lo constituye, sin duda, el ámbito de la **aviación civil**, donde El Reglamento (CE) 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, establece normas básicas comunes de obligado cumplimiento por todos los Estados miembros, para proteger a la aviación civil de actos de interferencia ilícita.

En su virtud, todas las personas, incluidos los miembros de las tripulaciones, deberán superar una comprobación de antecedentes personales antes de que les sea expedida una tarjeta de identificación que autorice el libre acceso a las zonas restringidas de seguridad. Igualmente, para personal con acceso a áreas sensibles para la seguridad, se establece un examen previo a la contratación que consistirá en establecer documentalmente la identidad de la persona, referir la formación y experiencia laboral y las posibles lagunas

durante al menos los 5 años precedentes, y exigir que la persona en cuestión firme una declaración en la que asegure que no tiene antecedentes penales en todos los Estados de residencia durante al menos los 5 años precedentes.

De acuerdo con este Reglamento, en España, la Instrucción SA-20 de la AESA, sobre "Evaluación de la idoneidad del personal en el ámbito de la Aviación Civil", establece el procedimiento para esta evaluación en los diferentes supuestos, los tipos delictivos que darán origen a un informe negativo y los mecanismos de defensa de los interesados frente a estos informes negativos.

Pero más aún: considerando que es imprescindible aumentar al límite la vigilancia del personal laboral en la lucha contra el terrorismo en los aeródromos, la Secretaría General de Transporte del Ministerio de Fomento dictó la Resolución de 9 de julio de 2019, que modifica la parte pública del Programa Nacional de Seguridad para la Aviación Civil, de forma que se mantienen las condiciones del examen previo a la contratación para personas que realizan su actividad fuera de las Zonas Restringidas de Seguridad (ZRS). Se endurecen, en cambio, para todo el personal, incluidos los miembros de las tripulaciones, que desarrolla su actividad accediendo a la ZRS del aeropuerto, introduciéndose una **comprobación de antecedentes reforzada** que incluye la información de inteligencia y de cualquier otro tipo de que dispongan las autoridades nacionales competentes, que estas consideren pertinente al objeto de determinar la idoneidad de la persona, y que puedan suponer un riesgo para la seguridad de la aviación civil. El mantenimiento de este requisito debe ser permanente y, en consecuencia, la comprobación de antecedentes reforzada se repetirá a intervalos regulares no superiores a doce meses.

En el ámbito de las **instalaciones nucleares**, el Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas, establece que aquellas deben disponer de un Registro del personal de la instalación y del de empresas contratadas que, por el ejercicio de las funciones encomendadas, precise acceder a áreas de la instalación o a informaciones sensibles desde el punto de vista de la protección física, quedando obligado el titular a mantenerlo actualizado y a informar al Ministerio del Interior, previamente a cualquier inscripción o baja en el Registro, para que se efectúen las comprobaciones necesarias en relación con los objetivos de protección física del material nuclear y de la instalación.

En este mismo sentido, merece destacarse la Orden PCI/168/2019, de 22 de febrero, por la que se publica el **Plan Nacional de Biocustodia**, aprobado por el Consejo de Seguridad Nacional, la cual establece que se determinarán los casos en los que sea necesaria una habilitación especial de seguridad para el personal con acceso directo, ya sea habitual, ocasional o temporal, a ciertos patógenos y toxinas relevantes, correspondiendo a la Comisión Nacional de Biocustodia recibir y tramitar la solicitud

de habilitaciones de seguridad por parte de instalaciones públicas y privadas, para trabajar con agentes biológicos relevantes, así como proponer a las autoridades competentes los puestos de trabajo que requieren habilitaciones de seguridad para el trabajo con agentes biológicos relevantes y acceso a información sensible relacionada en el territorio nacional.

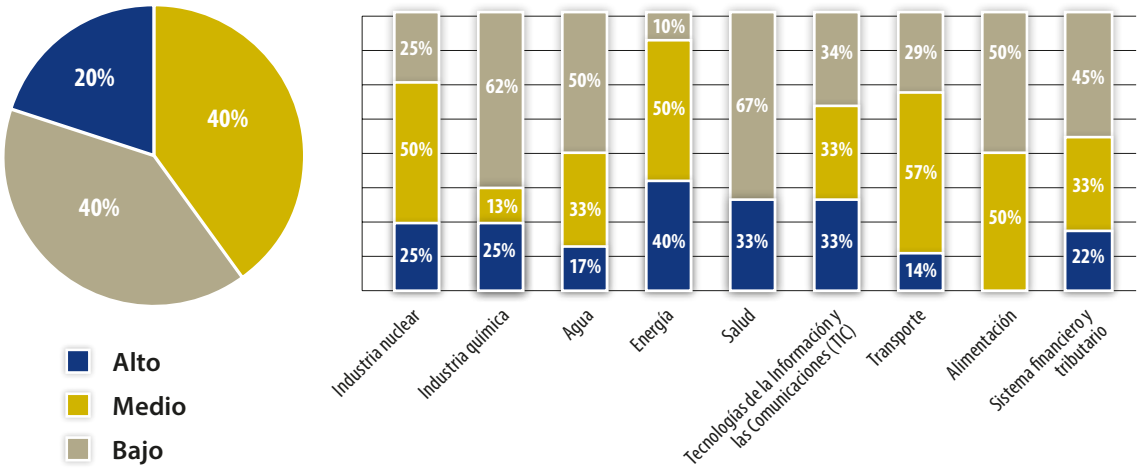
Con carácter general, la **Ley 5/2014, de Seguridad Privada**, Artículo 36.1.i), faculta a los directores de seguridad para llevar a cabo las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial. En este sentido, el artículo 14.3 dispone que las Fuerzas y Cuerpos de Seguridad podrán facilitar al personal de seguridad privada, en el ejercicio de sus funciones, informaciones que faciliten su evaluación de riesgos y consiguiente implementación de medidas de protección. Si estas informaciones contuvieran datos de carácter personal sólo podrán facilitarse en caso de peligro real para la seguridad pública o para evitar la comisión de infracciones penales.

2. SITUACIÓN EN EL ÁMBITO DE LAS INFRAESTRUCTURAS CRÍTICAS

Para analizar la percepción del fenómeno de la amenaza interna en el ámbito de los operadores críticos, se les envió un cuestionario a los Responsables de Seguridad y Enlace de los diferentes sectores estratégicos, a través de sus representantes en la mesa de coordinación del CNPIC. Las preguntas hacían referencia a diversos aspectos relacionados con la cuestión, su valoración del riesgo, instrumentos disponibles para afrontarlo y actitud de sus respectivas direcciones. Habida cuenta de que voluntariamente participaron en el estudio sesenta operadores críticos, el conjunto de sus respuestas, anónimas, con indicación únicamente del sector estratégico al que pertenece el encuestado, constituyen una muestra suficientemente representativa para una percepción real de la trascendencia del fenómeno. Por ello, es obligado agradecer también la proactividad de los RSE al implicarse en este estudio y llenarlo de contenido.

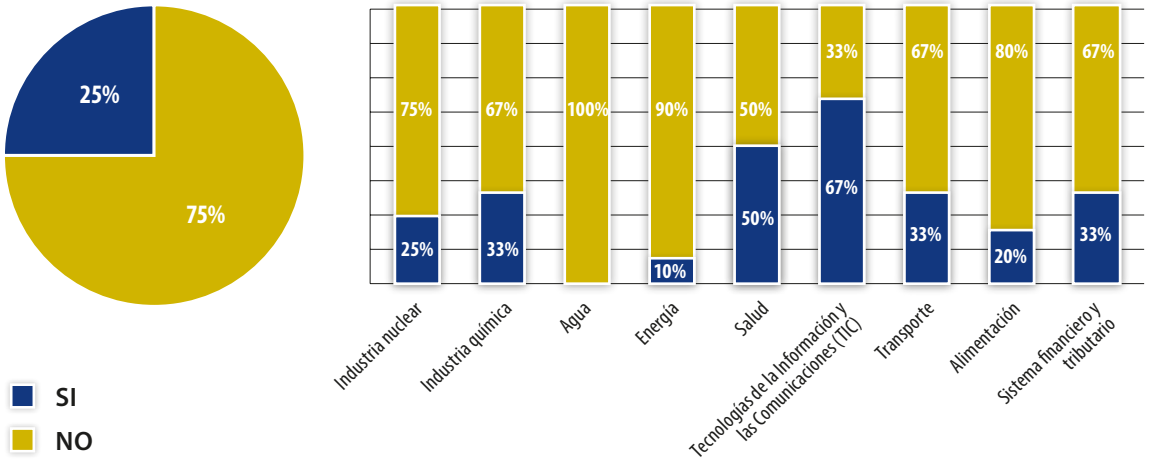
- VALORACIÓN DEL RIESGO. En primer lugar, el riesgo de que personal interno de la propia compañía o de sus proveedores participe, bajo cualquier motivación, en ataques contra sus activos se valora como **bajo** por un 40% de los participantes. Idéntico porcentaje lo valora como **medio** y sólo un 20% lo considera **alto**.

¿Cómo valora el riesgo de que personal interno de su compañía o de sus proveedores participe, bajo cualquier motivación, en ataques contra sus activos?



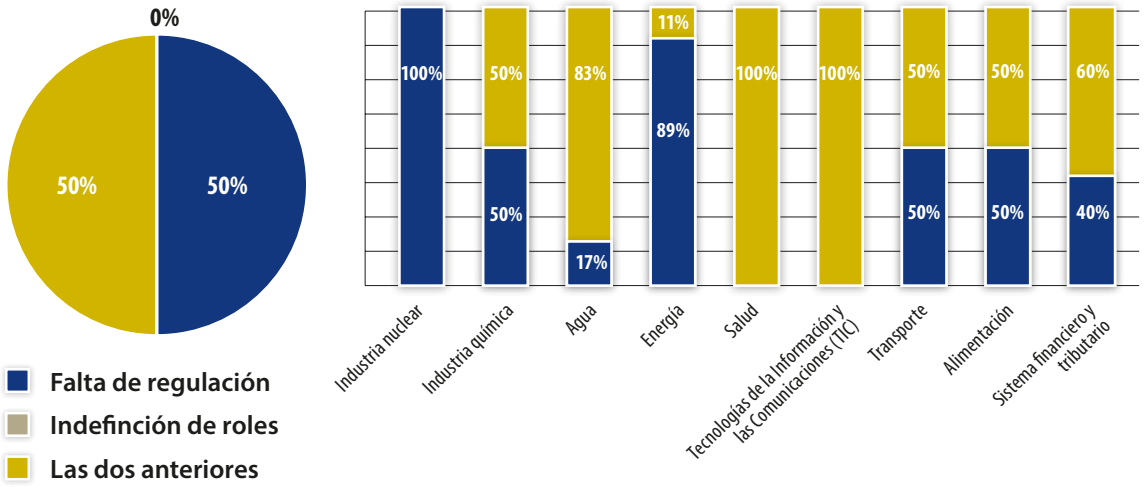
VERIFICACIONES DE PROBIDAD. El 75% de los operadores críticos consultados **no realizan oficialmente ninguna comprobación sobre la probidad de sus propios empleados**. El porcentaje sube hasta el 82% cuando se trata de verificar la probidad de empleados de terceros proveedores. Llama la atención que, precisamente en el sector de la energía, sólo el 10% de los intervinientes la realiza, y ninguno, cuando se trata de terceros proveedores.

¿Su compañía lleva a cabo verificaciones de la probidad de sus empleados?



- CAUSAS DE LA NO VERIFICACIÓN. En todos los casos, la razón esgrimida para explicar esta falta de comprobaciones es la **inexistencia de una regulación legal que las facilite**; en un 50% de los casos se añade, además, la indefinición de los roles y responsabilidades entre los distintos departamentos de la empresa.

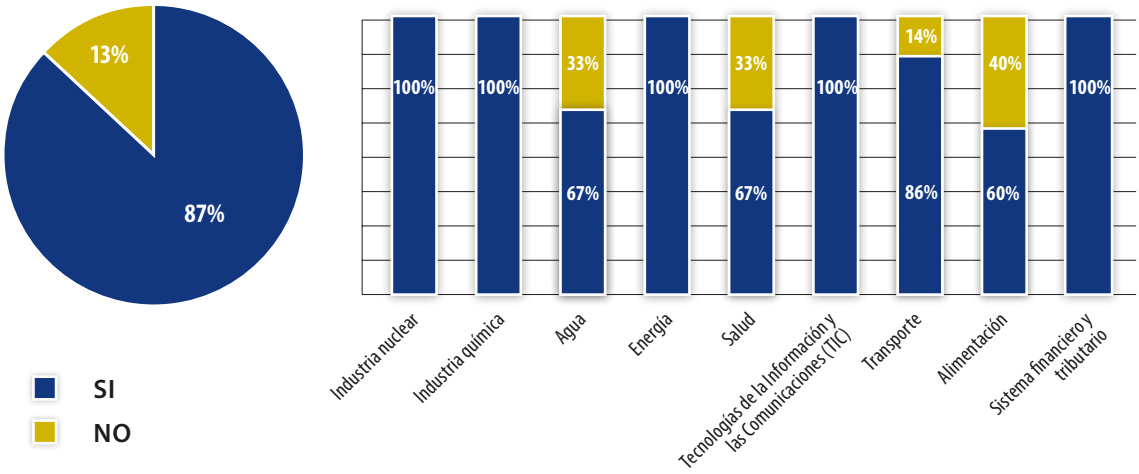
Razón de no llevar a acabo comprobaciones



En ocasiones, se alude también a la falta de medios para efectuar esas comprobaciones de antecedentes o al desconocimiento de los procedimientos. Incluso se plantea que no se hacen comprobaciones porque se ha valorado el riesgo de la amenaza interna como bajo. En cualquier caso, los propios departamentos de seguridad de las compañías asumen, en determinadas circunstancias y con sus propios medios, algún tipo de verificación de idoneidad, para lo cual implementan procedimientos específicos como consultas a las FCS (28%) o investigaciones internas (17%). No obstante, hay que destacar que un 55% no dispone de procedimientos de verificación.

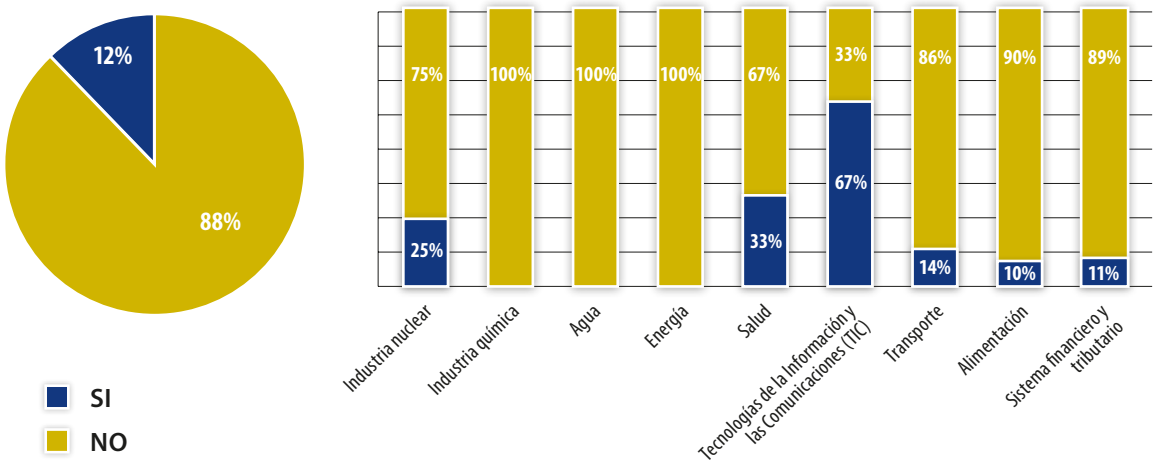
NECESIDAD DE REGULACIÓN. Resulta significativo que el 87% considera necesario disponer de un instrumento jurídico habilitante para despejar dudas sobre la posibilidad de realizar comprobaciones de probidad.

¿Considera necesario disponer de un instrumento jurídico habilitante para efectuar comprobaciones de probidad sobre el personal de la empresa o subcontratado?



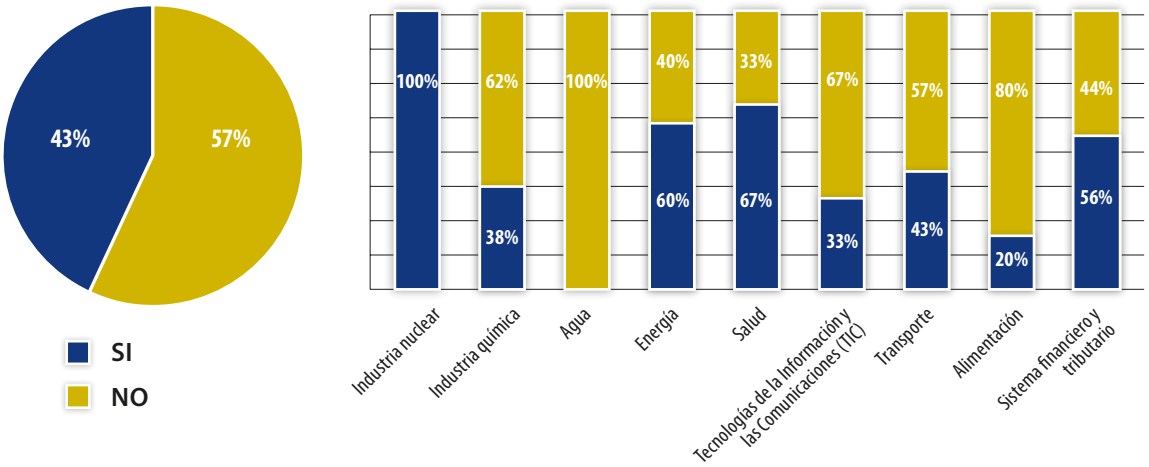
CLÁUSULAS EN LOS CONTRATOS. Por otra parte, **el 88% de las empresas no establece en sus contratos de personal**, o en los que suscribe con sus proveedores, **cláusulas con la exigencia de someterse a comprobaciones** de idoneidad y probidad para acceder a sus instalaciones o información.

¿Su compañía establece en sus contratos de personal, o en los que suscribe con sus proveedores, cláusulas con la exigencia de someterse a comprobaciones de idoneidad y probidad para acceder a sus instalaciones?



DEPENDENCIA DE PROVEEDORES. Una circunstancia a tomar en consideración es que el 43% de las compañías que colaboraron en el estudio, se encuentran en ocasiones con una **dependencia excesiva de algún proveedor** para el que no disponen de alternativa, lo que dificulta ejercer sobre ellos un adecuado control de seguridad. Esta circunstancia tiene especial incidencia en los sectores de la salud e industria nuclear y muy notable en los sectores de la energía y sistema financiero y tributario.

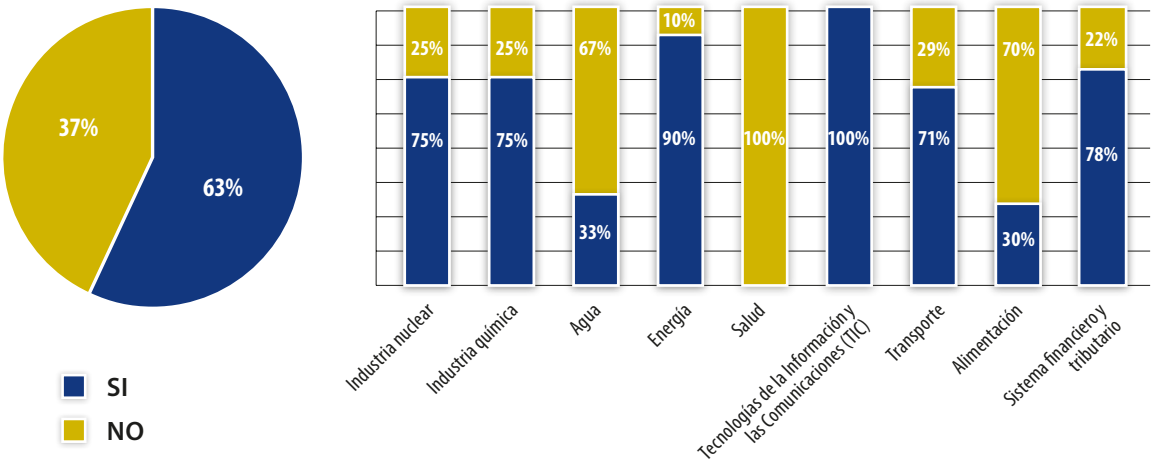
¿Su compañía se encuentra en ocasiones con una dependencia excesiva de algún proveedor para el que no dispone de alternativa?



En estos casos, se trata de servicios de mantenimiento súper especializados, así como de servicios de gestión de las tecnologías de la información y la comunicación, en los que el monopolio en la prestación provoca un cierto grado de impotencia a la hora de implantar medidas de control de seguridad. Habida cuenta de que se hace primar la continuidad del negocio, la fiabilidad de los trabajadores se deja en manos de las empresas contratistas.

INTERPRETACIONES RESTRICTIVAS. Resulta significativo que el 63% de los RSE encuestados tiene la percepción de que, en ocasiones, **la interpretación que hacen sus departamentos jurídicos sobre determinadas normas restringe en exceso su margen de actuación**, llegando a perjudicar la capacidad de autoprotección de su empresa, en beneficio de su seguridad frente a posibles reclamaciones.

¿Considera que algunas interpretaciones excesivamente restrictivas de los departamentos jurídicos, en cuanto a su margen de actuación, pueden llegar a perjudicar la capacidad de autoprotección de su empresa?



INCONGRUENCIA NORMATIVA. Todos los sectores analizados, con la única excepción del de la salud, dan cuenta de una **afectación a normas sectoriales que exigen la publicación de información sensible para la seguridad** o impiden la perfecta ejecución de la política de seguridad de la empresa (por razones medioambientales, de transparencia, de protección de datos...), hasta el punto de resultar incompatibles con las medidas de seguridad exigibles a un operador crítico.

3. ANÁLISIS JURÍDICO DE LA SITUACIÓN

La Directiva 2008/114/CE del Consejo de la UE, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas (ICE) y la evaluación de la necesidad de mejorar su protección, en el considerando 6 de su Preámbulo establece que: "*La responsabilidad principal y última de proteger las ICE corresponde a los Estados miembros y a los propietarios u operadores de tales infraestructuras*". Esta Directiva surge en el marco de un Programa Europeo de Protección de las Infraestructuras Críticas, basado en un planteamiento que tiene en cuenta todo tipo de riesgos, pero dando preferencia a la lucha contra amenazas terroristas; en consecuencia, su fin principal es contribuir a la protección de la población.

Al transponer esta Directiva, la Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas, desarrolla, ampliamente, el concepto de "*Protección*", definiéndola como el "…*conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia*." Esta responsabilidad es atribuida, de manera directa, tanto a las administraciones públicas competentes, como a los operadores y gestores de dichas infraestructuras.

La falta de atención en el ejercicio material de esta labor de protección podría tener consecuencias penales para quienes la tienen encomendada, toda vez que el actual artículo 31 bis del Código Penal establece que: "… las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control atendidas las concretas circunstancias del caso".

Ha de tenerse presente que, actualmente, el cumplimiento normativo en el ámbito penal es una nueva exigencia de política de prevención general, para evitar la comisión de delitos que anteriormente podrían quedar enmascarados y menos perseguidos por la falta de responsabilidad penal de las sociedades. Hasta ahora y sin esta evolución de nuestro Código Penal, había que probar el dolo en la sociedad para derivar una responsabilidad civil. Con el "*Corporate Compliance*" la carga de la prueba se ha invertido y será la empresa quien deberá probar el cumplimiento del deber de diligencia en la aplicación del modelo de prevención y gestión para que no se le pueda derivar responsabilidad penal alguna.

En todo caso, es evidente que habría una clara responsabilidad civil a la vista del contenido de los artículos 1902 y siguientes del Código Civil, relativos a las obligaciones que nacen de la culpa y negligencia, que vienen a concretarse en que "*El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causa-*

do". En definitiva, la falta de atención sobre la idoneidad y probidad del personal que tiene acceso a áreas o informaciones sensibles de un operador crítico, podría hacer recaer sobre éste una responsabilidad civil o incluso penal, por culpa *"in eligendo"* o *"in vigilando"*.

Tratándose de infraestructuras críticas con instalaciones que pueden llegar a constituir un peligro potencial para la población, y siendo compartida la responsabilidad de su protección por el Estado y por los propios operadores, la más elemental medida de control, en línea con las ya adoptadas en otros ámbitos similares, sería la **comprobación previa por los operadores, con el apoyo del Ministerio del Interior, de la idoneidad** de las personas antes de darles acceso a áreas o informaciones sensibles de sus organizaciones o de las propias infraestructuras críticas que operen. A estos efectos, la idoneidad estaría determinada por la carencia de antecedentes penales relevantes en relación con la seguridad de la infraestructura protegida. En función del nivel de acceso a espacios críticos, la verificación de la idoneidad debería incluir el apoyo de informes de inteligencia de las Fuerzas y Cuerpos de Seguridad para analizar otras circunstancias de la persona que pudieran tener relación con la seguridad de la infraestructura crítica protegida.

Como quiera que el cumplimiento de este requisito debe ser permanente, estas comprobaciones de idoneidad deben llevarse a cabo con periodicidad, debiendo establecerse, como medida complementaria, los efectos de una evaluación negativa, en cuanto a la posibilidad de una modificación del puesto de trabajo o, incluso, de extinguir el contrato laboral de los operadores con aquellas personas que devinieran un elemento potencial de riesgo para dichas instalaciones.

La exigencia de este requisito no puede entenderse como discriminatoria para los trabajadores afectados, toda vez que, en base a su finalidad y efectos pretendidos, puede considerarse amparada por la doctrina del Tribunal Europeo de Derechos y Humanos y del Tribunal Constitucional, puesta de manifiesto en diversas sentencias. En particular, para el primero de ellos, el Convenio Europeo para la Protección de los Derechos y de las Libertades Fundamentales no prohíbe toda diferencia de trato en el ejercicio de los derechos y libertades, de forma que **no toda desigualdad constituye necesariamente una discriminación** y entiende que la igualdad es sólo violada si la desigualdad está desprovista de una justificación objetiva y razonable; la existencia de dicha justificación debe apreciarse en relación a la finalidad y efectos de la medida considerada, debiendo darse una relación razonable de proporcionalidad entre los medios empleados y la finalidad perseguida.

Por su parte, el Tribunal Constitucional, sobre arbitrariedad y discriminación, en su STC 125/2003, de 19 de junio, señala que: "*configurar supuestos de hecho de la norma de modo que se dé trato distinto, a personas que, desde todos los puntos de vista legítimamente adoptables, se encuentren en la misma situación o, dicho de otro modo, impidiendo que se otorgue relevancia jurídica a circunstancias que, o bien no pueden ser jamás tomadas en consideración por prohibirlo así la propia Constitución, o bien no guardan relación alguna con el sentido de la regulación que, al incluirlas, incurre en arbitrariedad y es por eso discriminatoria*".

Por todo ello ha de entenderse que, en el caso que nos ocupa, la exigencia de someterse a comprobaciones de antecedentes penales no sería una conducta discriminatoria, más aún cuando se produce atendiendo a las previsiones de protección establecidas por la Directiva europea sobre la identificación y designación de las infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Por otra parte, la medida contemplada no resulta novedosa, toda vez que son numerosos los casos en los que la legislación española recoge la legitimidad de solicitar el certificado de antecedentes penales tanto para el acceso a la función pública como en el sector privado, para contratar con el sector público o para el ejercicio de determinadas profesiones o actividades (ejercicio de la abogacía, representantes de empresas de seguridad privada o profesionales de seguridad privada, juego, armeros, cuidado de menores…). En cualquier caso, no sólo la exigencia de certificaciones sobre antecedentes penales, sino incluso la imposición de autorización previa para el ejercicio de determinadas actividades tuteladas por la Administración está presente en numerosas normas, como ejemplo de requisitos personales y específicos exigibles.

Como ya hemos visto, en ciertos ámbitos se ha establecido la condición de superar pruebas de idoneidad para acceder a determinados puestos. En este sentido, resulta paradigmática la situación en el ámbito de la aviación civil, donde el Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil, señala, en su punto 11.1, que: "*Las personas que practiquen controles, controles de acceso u otros controles de seguridad o sean responsables de ellos serán contratadas, formadas y, cuando proceda, certificadas de modo que quede garantizada su idoneidad para el puesto y su capacidad para llevar a cabo las tareas que se les asignen*". En el Reglamento Nº185/2010 de la Comisión de 4 de marzo de 2010, se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea; en particular, se recoge la prohibición de expedir tarjetas de identificación, como miembros de una tripulación o como personal de un aeropuerto en todas sus zonas, a personas que no hayan superado un control de antecedentes personales. Además, se procederá a la retirada de la tarjeta de identificación con carácter inmediato a toda persona que no supere los controles de antecedentes personales. Este control incluye los posibles antecedentes penales en todos los Estados de residencia durante, al menos, los 5 años precedentes. Sin duda, ésta constituye una herramienta legal para impedir el acceso a determinadas profesiones a personas con ciertos antecedentes penales previos.

En todo caso, el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, establece en su artículo 3.1.c) que "*los derechos y obligaciones concernientes a la relación laboral se regulan… por la voluntad de las partes, manifestada en el contrato de trabajo, siendo su objeto lícito y sin que en ningún caso puedan establecerse en perjuicio del trabajador condiciones menos favorables o contrarias a las disposiciones legales…*". Igualmente, dispone en su artículo

4.2.c) que los trabajadores tienen derecho "*a no ser discriminados directa o indirectamente para el empleo, o una vez empleados, por razones de sexo, estado civil, edad dentro de los límites marcados por esta ley, origen racial o étnico, condición social, religión o convicciones, ideas políticas, orientación sexual, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español*", condiciones entre las que no se hace referencia a los antecedentes penales.

En relación a los posibles argumentos en la afectación de la privacidad y la protección de los datos, el artículo 6.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, valida el consentimiento del afectado para el tratamiento de sus datos personales, siempre que se trate de una "*manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*". Respecto a este consentimiento, el artículo 6.3 establece que "*no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual*"; *a sensu contrario*, podrá supeditarse cuando la finalidad del tratamiento guarde relación con el control de la actividad contractual.

Por otra parte, el artículo 10 de la misma LO 3/2018, dispone que "*el tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas,* **para fines distintos de los de prevención***, investigación, detección o enjuiciamiento* **de infracciones penales o de ejecución de sanciones penales***, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal"*. En el caso que nos ocupa, es evidente que los datos sobre antecedentes penales se requieren para una labor preventiva de acciones deliberadas contra infraestructuras críticas, en el marco del sistema de protección establecido por la Directiva 2008/114 y la Ley 8/2011.

Hay que destacar que el RGPD, en su artículo 2.2 impone una clara limitación en su ámbito de aplicación: *"El presente Reglamento no se aplica al tratamiento de datos personales: … d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención*". En cualquier caso, el artículo 6 previene que el tratamiento de los datos será lícito "… *c) cuando es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"*. A mayor abundamiento, en su artículo 23.1 establece que *"El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos…, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pú-*

blica; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención…"

Respecto al posible impacto de esta medida en materia de protección de datos de los trabajadores en el ámbito laboral, conviene significar que el "*Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores*", de la Oficina Internacional del Trabajo de las Naciones Unidas, recoge que los empleadores no deberían recabar datos personales de los trabajadores que se refieran, entre otros aspectos, a los antecedentes penales. Sin embargo, entiende que, "*en circunstancias excepcionales, el empleador podría recabar este tipo de datos, siempre y cuando éstas guarden una relación directa con una decisión en materia de empleo y se cumplan las disposiciones de la legislación nacional*".

En definitiva, **se puede afirmar que el contrato de trabajo, o el acceso al mismo, puede someterse al cumplimiento de una o varias condiciones –ya sean previas o sobrevenidas– pudiendo extinguirse mediante una condición que podríamos denominar resolutoria; o no llegando a formalizarse, en el caso de la estipulación de una cláusula de condición "suspensiva", si ésta no llegará a consumarse o materializarse**. A este respecto, la Jurisprudencia viene siendo pacífica al aceptar que, para que resulte eficaz la condición, como causa extintiva de un contrato o precontrato, es necesario que no sea contraria a las leyes ni a la moral y al orden público; que no sea de imposible cumplimiento y que no constituya abuso de derecho manifiesto por parte del empresario. Visto lo anterior, será válida la condición que supedite la eficacia del contrato a la superación por el trabajador de ciertos exámenes o pruebas de aptitud iniciales o de carácter periódico, para acceder a determinadas zonas de una instalación o a determinadas informaciones sensibles de una empresa.

Es obvio que estas medidas, tanto la comprobación previa de antecedentes como el mantenimiento de esta condición en el tiempo, pueden y deben aplicarse también a los empleados de terceros, estableciendo las correspondientes cláusulas en la contratación de proveedores por el operador crítico, para velar por la probidad de quienes puedan tener acceso a áreas o informaciones sensibles.

4, CONCLUSIONES Y RECOMENDACIONES

1. La presencia de la denominada "amenaza interna" debe considerarse uno de los riesgos a los que están sometidas las infraestructuras críticas. Los expertos alertan de que las organizaciones terroristas siguen considerando a los elementos internos como un recurso potencialmente útil para facilitar la planificación de ataques. Por tanto, es necesario **fomentar una adecuada cultura de seguridad entre los operadores críticos, con objeto de que valoren este riesgo en su justa medida**, de acuerdo con su posibilidad real de ocurrencia y no mediante la contemplación de sucesos previamente acontecidos.

2. La mitigación de este riesgo precisa de una acción conjunta de los responsables de la protección de las infraestructuras críticas, Estado y Operador, a la que ambos deben contribuir en el marco de sus respectivas atribuciones. **Corresponde a los operadores desarrollar una adecuada estrategia de seguridad** e implementar aquellas medidas de protección integral que eleven su nivel de seguridad frente a riesgos de cualquier naturaleza. Por su parte, **corresponde al Estado desarrollar un marco normativo adecuado** para evitar la aparición de espacios de impunidad de cualquier orden y facilitar a los operadores el acceso a servicios de seguridad con garantía de calidad.

3. La responsabilidad que recae sobre los operadores críticos les exige mantener una **adecuada política de recursos humanos**, enfocada a minimizar los posibles riesgos que pudieran nacer de la amenaza de sufrir o causar un ilícito penal, asumiendo que de ellos se derivan responsabilidades de todo tipo, tanto por *culpa in eligendo* al seleccionar a su personal, como por *culpa in vigilando* al no ejercer sobre ese personal las medidas de control necesarias para evitar la comisión de tales ilícitos penales.

4. Esta política de recursos humanos debería incluir, como elemental medida de protección, la **verificación de los antecedentes penales** de cualquier empleado, directo o indirecto, que tenga acceso a áreas o informaciones sensibles de instalaciones u operadores críticos, impidiendo su presencia cuando concurran circunstancias objetivas que pongan de manifiesto su condición de amenaza potencial para la integridad de la instalación o la continuidad de su actividad.

5. Tanto la solicitud de antecedentes penales, como la emisión de las correspondientes certificaciones, se encuentran debidamente reguladas por normativa específica en la materia, estableciendo, al efecto, los procedimientos a seguir, así como los organismos, funcionarios y personas autorizadas para acceder al Registro Central de Penados. En este espacio alcanza su verdadero valor la **cooperación entre los operadores críticos y el Ministerio del Interior**.

6. Existen en nuestro ordenamiento jurídico **numerosos ejemplos**, tanto en el ámbito público como en el privado, **de la exigencia de carecer de antecedentes penales o de acreditar buena conducta** para acceder a determinados puestos de trabajo, sin que el requerimiento de antecedentes penales en tales supuestos implique afectación a la protección de datos en el ámbito laboral o discriminación de ningún tipo.

7. La **justificación legal** para emprender acciones encaminadas a una contratación responsable de empleados en el ámbito de las infraestructuras críticas, está **contenida implícitamente en diversas normas** de nuestro ordenamiento jurídico sin que exista ninguna que explícitamente lo prevea. Por ello, tratando de proteger los intereses de sus empresas frente a posibles reclamaciones en el ámbito laboral, los departamentos jurídicos acuden con frecuencia a interpretaciones que restringen el uso de estos mecanismos.

8. No obstante, dadas las garantías de seguridad requeridas para la protección de este tipo de instalaciones, resulta, más que conveniente, **necesaria, la exigencia de carecer de antecedentes penales** para acceder a determinadas áreas o informaciones en el ámbito de las infraestructuras críticas, con el fin de contribuir no sólo a su seguridad específica, sino también, a la seguridad pública en su conjunto.

9. **Corresponde a los Operadores Críticos**, a través de los Planes de Seguridad del Operador y Planes de Protección Específicos, establecer la política de seguridad del operador en materia de filtros al personal propio o de terceros proveedores, así como **la delimitación indubitada de aquellos espacios a los que el personal sólo podrá acceder previa verificación de sus antecedentes** penales u otras comprobaciones de conducta.

10. **El Estado debe adoptar las medidas reguladoras pertinentes para ofrecer seguridad jurídica a los operadores** en su labor de verificación de la idoneidad del personal que pueda tener acceso a sus activos. En particular, debe diseñar un **procedimiento ágil y seguro para que el Ministerio del Interior pueda apoyar al operador en la comprobación de los antecedentes** penales de los empleados propios y de terceros proveedores, así como de otras circunstancias objetivas que den lugar a la prohibición de acceso a determinadas áreas o informaciones.

11. Merece una especial atención el hecho de que, ocasionalmente, los operadores críticos se encuentran en una **posición de dependencia respecto a proveedores de servicios para los que no existe alternativa**. En estos supuestos podría valorarse una certificación previa de la empresa proveedora en base a una política de control de su propio personal, acorde con los requerimientos establecidos para el operador.

12. Como quiera que la amenaza interna puede provenir también de **empleados incompetentes o negligentes**, los planes de seguridad del operador deben hacer referencia a su política de formación y control del personal para velar por su más correcta capacitación técnica y desempeño profesional. Igualmente, deben contemplar acciones para minimizar el riesgo de que **personal con privilegios de acceso** viole las normas de seguridad establecidas.

13. La Administración debe llevar a cabo un esfuerzo para **eliminar las posibles incongruencias normativas** que desvirtúan la especial protección que indudablemente quiere prestar a las infraestructuras críticas y servicios esenciales. Su consideración de excepcionalidad a la hora de exigir a los operadores críticos medidas de protección singulares requiere también un tratamiento de excepcionalidad en relación con otras normativas que puedan colisionar con sus necesidades de seguridad.

5. PROPUESTA DE ACCIONES

A la vista de los datos recogidos en este informe y su valoración, desde la FUNDACIÓN BORREDA, se propone desarrollar una estrategia sustentada en tres acciones regulatorias complementarias, simultáneas en su concepción y con entrada en vigor escalonada en el tiempo de acuerdo a sus respectivos ritmos de tramitación:

5. 1. Reforma de la Ley 8/2011

La aparición de la Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión y su correspondiente transposición mediante el Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información, parecen aconsejar una reforma de la Ley 8/2011, por la que se establecen medidas para la protección de las Infraestructuras Críticas, para armonizar la regulación de ambos sectores, al margen de incorporar algunos aspectos que la experiencia adquirida desde su promulgación aconsejan actualizar.

Esta deseable reforma constituiría una excelente oportunidad para establecer con claridad algunas cuestiones que se refieren al objeto de este informe:

- **Exigencia de superar una comprobación de idoneidad**[1], referida a la carencia de antecedentes penales u otros informes de conducta, para todo el personal perteneciente a la propia empresa, o a terceros proveedores, que precise acceder a áreas o informaciones sensibles de la organización, estableciendo, en su caso, el nivel de alcance de estas comprobaciones en función de los ámbitos de riesgo identificados. El cumplimiento de esta obligación correspondería a los Operadores Críticos, con el apoyo del Ministerio del Interior.

- **Obligación para los Operadores Críticos de identificar y delimitar los espacios o ámbitos de riesgo de su organización en los que se exige una verificación de idoneidad** que incluya comprobaciones de antecedentes penales, u otros informes de conducta, a toda persona que deba acceder a ellos para desempeñar su función.

- Obligación para los Operadores Críticos de **elaborar y mantener registros del personal** propio y de terceros proveedores autorizado para acceder a estas zonas y ponerlos a disposición del CNPIC para el ejercicio de su función inspectora. La incorporación de nuevas personas al registro exigirá, en todo caso, la previa comprobación de su idoneidad en los términos descritos, debiendo comunicarse las bajas al CNPIC tan pronto como se produzcan, indicando las causas.

[1] Excepto el último punto, el resto de los propuestos pueden ser establecidos en una Instrucción de la SES. No obstante, su regulación por Ley vendría a despejar dudas y facilitar su implantación.

- Establecer con toda claridad que las actuaciones, comunicaciones, archivos, registros y documentos relativos al diseño, establecimiento y aplicación de las medidas de seguridad que afecten a las infraestructuras críticas y a la protección de los servicios esenciales, o cualquier otro tipo de información que comprometa la seguridad de estas instalaciones, tendrán la consideración de **información que afecta a la Seguridad del Estado** a los efectos de lo previsto en el apartado 5 del artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Se pretende eliminar así el efecto que viene produciéndose como consecuencia de la incongruencia normativa que supone aplicar a las infraestructuras críticas, para las que se exige el cumplimiento de unos requisitos especiales de seguridad, la normativa general diseñada para proteger otros bienes jurídicos no directamente relacionados con la Seguridad del Estado, tales como los que se señalan a continuación:

- Informaciones publicadas en plataformas de internet (Google Earth, Marine Traffic, webs de las Autoridades Portuarias…)
- Publicidad de los informes de seguridad de las empresas SEVESO, que contienen información sensible de la empresa
- Autorizaciones medioambientales y planes de autoprotección y emergencias
- Obligaciones de transparencia en la documentación oficial
- Protección de datos personales, que limitan la gestión de medidas de seguridad, especialmente los análisis de riesgos
- Permisos y licencias municipales de obra civil
- Exceso de información en licitaciones públicas

5. 2. Elaboración de una norma específica del Ministerio del Interior

Con independencia de que se proceda a una reforma de la Ley 8/2011 en el sentido indicado en el punto anterior, se considera que existen ya en nuestro ordenamiento jurídico suficientes elementos para proceder a regular las verificaciones de idoneidad del personal que precise acceder a áreas o informaciones sensibles de los operadores críticos. En este sentido, una norma del Ministerio del Interior, con el rango que se estime pertinente, regulando el procedimiento para proceder a la comprobación de los antecedentes penales del personal o de terceros proveedores y establecer la forma en que deba materializarse el apoyo del Ministerio al Operador, tendría la virtud de constituir el primer instrumento normativo que se ocupe de este problema, despejando así las dudas manifestadas por

los departamentos legales de las empresas ante la falta de instrumentos jurídicos de aplicación.

Esta norma debería tener en cuenta, entre otros, los siguientes aspectos:

- Definir inequívocamente el concepto de amenaza interna que da lugar a acciones de verificación de idoneidad.
- Atribuir al operador la responsabilidad de identificar los espacios y accesos que requieren verificación de idoneidad.
- Establecer un procedimiento ágil y seguro para las verificaciones, en el que se asignen tareas tanto al operador como a la administración.
- Detallar las concretas comprobaciones a efectuar en sus bases por el Ministerio del Interior, más allá de los simples antecedentes penales.
- Facilitar a los operadores críticos la contratación segura de servicios, poniendo a disposición de sus proveedores un procedimiento para que éstos puedan verificar anticipadamente la idoneidad de su personal.
- Elaborar un catálogo de delitos que impliquen automáticamente la exclusión de las zonas de acceso restringido.
- Implantar mecanismos para el estudio de casos dudosos que incluyan la participación del cuerpo responsable del Plan de Apoyo Operativo.
- Establecer la vigencia de las verificaciones.
- Regular la llevanza de los registros de personal necesarios.

5.3. Elaboración por el cnpic de una guía de buenas prácticas en la prevención de la amenaza interna por los operadores críticos (y proveedores de servicios esenciales)[2]

Esta Guía, que debería publicarse con carácter inmediato, recogería las recomendaciones del CNPIC sobre cuestiones relativas a las condiciones de contratación de personal propio y proveedores y medidas para el control de todo tipo de personal que accede a recursos sensibles de la organización, así como mecanismos para prevenir acciones malintencionadas o inconscientes y para restablecer la continuidad del servicio afectado. A título de ejemplo, se enumeran las siguientes:

[2] Una cuestión a dilucidar es si toda esta regulación debe afectar, no sólo a los operadores críticos, sino también a los proveedores de servicios esenciales.

- Implantación de políticas de selección del personal que incluyan la verificación de la formación y experiencia profesional, así como la investigación de las posibles "lagunas" existentes durante, al menos, los cinco años precedentes.

- Establecimiento de planes de sensibilización y formación para personal de cualquier tipo que acceda a áreas o informaciones sensibles del operador y sus infraestructuras críticas, tales como:

  - Detección de actitudes sospechosas del personal

  - Modus operandi habituales en la comisión de delitos

  - Repercusiones del incumplimiento de pautas de seguridad

  - Posibles sanciones (para empresa y empleados)

  - Errores humanos más habituales

  - Riesgos del uso inadecuado de los dispositivos conectados

- Disposición de protocolos para asegurar el mantenimiento de la aptitud técnica necesaria e implantación de medidas de seguridad específicas para todo el personal, incluido aquel con privilegios de acceso, en orden a prevenir daños por negligencia o imprudencia.

- Adopción de medidas para el control de proveedores con acceso a los activos de la empresa, especialmente cuando se trate de proveedores con los que se mantiene una situación de excesiva dependencia.

- Aplicación de medidas de seguridad básicas para minimizar los riesgos, enfocando la protección a:

  - La gestión de activos

  - La seguridad de las operaciones

  - La gestión de incidentes tanto de carácter intencionado como accidental

  - El control de acceso a sistemas y aplicaciones por parte de todos los empleados, estableciendo diferentes niveles de acceso, en función de las necesidades reales.

- Implantación de equipos y protocolos de comunicación que garanticen un tratamiento adecuado de los posibles incidentes y minimicen su impacto social, a la vez que favorecen la continuidad del servicio.

- Concienciación de los departamentos de seguridad, y a través de ellos de todo el personal, para prestar especial atención a las personas con acceso a espacios sensibles, para detectar posibles cambios de actitud que pudieran anunciar procesos de radicalización.

- Identificación de factores y comportamientos que ayuden a detectar conductas sospechosas y prevenir la amenaza interna.

- Establecimiento de medidas de coordinación con otros operadores del sector y entre diferentes áreas de la misma compañía a fin de garantizar el mejor control del personal.

- Revisión periódica de credenciales de acceso y privilegios de usuarios, estableciendo por defecto el principio de privilegios mínimo y limitando la utilización de usuarios genéricos en aplicaciones. Igualmente, establecer una política de caducidad de contraseñas y acreditaciones.

- Identificar bases de datos sensibles, en cualquier soporte, y aplicar controles específicos sobre ellas.

- Establecer acuerdos de confidencialidad con empleados y proveedores, asociados a un sistema de penalizaciones por incumplimiento.

- Auditar periódicamente los sistemas y procedimientos de seguridad para verificar su eficacia y correcta aplicación. Llevar a cabo pruebas y ataques simulados para entrenar respuestas.

- Desarrollar procedimientos para la investigación de incidentes de seguridad (metodología, fuentes de información, competencias, medidas preventivas…)

Estudio: La amenaza interna en el ámbito de las Infraestructuras Críticas
Edición: 2019
Edita:Fundación Borredá
Registro de Fundaciones nº 1.461 (Orden ECD/1304/2012 de 16 de abril, BOE nº 118)
Calle Don Ramón de la Cruz, 68 2º Derecha. 28001 Madrid. Tel + 34 91 309 04 54
www.fundacionborreda.org

EN LA REALIZACIÓN DEL DOCUMENTO HA PARTICIPADO UN EQUIPO FORMADO POR LOS SIGUIENTES MIEMBROS:

COORDINADOR GENERAL
César Álvarez Fernández

COMISIÓN TÉCNICA
Laura Borredá
Eva Martín
Enrique González
Ana Borredá

MAQUETACIÓN
Macarena Fdez. López

Con la colaboración del

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

La Fundación Borredá lleva a cabo sus fines gracias a la contribución de sus socios protectores

Accenture Security · AXIS COMMUNICATIONS · Deloitte. · dormakaba · everis · gmv · S21sec · SAIMA SAIMA SEGURIDAD, S.A. · TECOSA · Telefónica


FUNDACIÓN
BORREDÁ
al servicio de la seguridad