El deber de la Intervención Local de revisar los controles de seguridad de la información. La metodología de los controles básicos de ciberseguridad de la GPF-OCEX 5313 como instrumento adecuado para cumplir con esta responsabilidad.

Juan Javier González Rodríguez
Viceinterventor de la Diputación de Granada

Revista Auditoría Pública nº 86
Diciembre 2025. Páginas: 101-108

Resumen: La generalización de la administración electrónica ha desplazado el riesgo material hacia los sistemas de información de las entidades locales, haciendo de la ciberseguridad un componente ineludible del control interno. La Intervención Local no solo está habilitada, sino obligada normativamente a verificar la seguridad y fiabilidad de los sistemas que soportan la información económico-financiera, de conformidad con el marco jurídico del control interno local (R.D. 424/2017) y el estatuto de los Habilitados Nacionales (R.D. 128/2018). Para este cometido, se propone la GPF–OCEX 5313 –centrada en ocho Controles Básicos de Ciberseguridad (CBCS) y alineada con el ENS– como metodología adecuada para cumplir esa responsabilidad, por su sencillez, objetividad y comparabilidad. La guía permite obtener índices de madurez (0–100%), que permiten cuantificar el estado de la seguridad de los sistemas de información de la entidad, posibilitando a su vez la comparación con otras entidades, la medición de la evolución a lo largo del tiempo y cuantificar el esfuerzo a realizar para alcanzar los requerimientos mínimos.

Palabras Clave: Intervención Local; Controles Básicos de Ciberseguridad; GPF–OCEX 5313; Esquema Nacional de Seguridad (ENS); Auditoría basada en riesgos.

Abstract: The widespread adoption of e-government has shifted material risk towards the information systems of local entities, making cybersecurity an essential component of internal control. Local Audit Offices are not only empowered but also legally required to verify the security and reliability of the systems that support financial and accounting information, in accordance with the legal framework of local internal control (Royal Decree 424/2017) and the statute of local government auditors and treasurers (Royal Decree 128/2018). For this purpose, GPF–OCEX 5313 –focused on eight Basic Cybersecurity Controls (CBCS) and aligned with the National Security Framework (ENS)– is proposed as the appropriate methodology to fulfill this responsibility, due to its simplicity, objectivity, and comparability. The guide enables the calculation of maturity indices (0–100%), which quantify the security status of the entity's information systems, while also allowing comparisons with other entities, measuring progress over time, and assessing the effort required to meet minimum requirements.

Keywords: Local Intervention; Basic Cybersecurity Controls; GPF–OCEX 5313; National Security Scheme (ENS); Risk-based Audit.

1. Implantación de la Administración electrónica en las entidades locales y consecuencias para la ciberseguridad.

El concepto "administración electrónica" proviene de la Comisión Europea, que en 2003 la definió como "el uso de las tecnologías de la información y las comunicaciones en las Administraciones Públicas, combinado con cambios organizativos y nuevas amplitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas".[1]

Pese a que ya en 2007 la prestación de servicios públicos a través de medios digitales fue prevista legalmente, en la Ley 11/2007, de 22 de junio de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, el verdadero impulso a la administración electrónica en España no se produjo hasta la aprobación de las leyes 39/2015, del Procedimiento Administrativo Común, y la 40/2015, de Régimen Jurídico del Sector Público. Las mismas obligan a las Administraciones Públicas a tramitar electrónicamente, a garantizar la interoperabilidad y a proteger la información. Estas leyes se desarrollan mediante el Real Decreto 203/2021, que regula el funcionamiento del sector público por medios electrónicos, y se complementan con las prescripciones necesarias en cuestión de interoperabilidad y seguridad, recogidas en el Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI), aprobados por los reales decretos 311/2022, de 3 de mayo 23, y 4/2010, de 8 de enero, respectivamente, y en las correspondientes normas técnicas de desarrollo.

Esta transformación digital de las entidades locales amplía la exposición a riesgos cibernéticos. De acuerdo con Olano Salvador (2024), las ciberamenazas más utilizadas contra el sector público son:

- Software malicioso (malware): Bajo esta categoría se engloban múltiples tipos de programas diseñados con fines ilícitos, entre los que destacan los virus, gusanos, troyanos, adware y spyware. Su finalidad puede ir desde la filtración de datos hasta la alteración del funcionamiento de los sistemas, pasando por la instalación de puertas traseras para un acceso persistente.

- Ransomware: Representa una modalidad específica de malware que cifra los archivos y sistemas de la organización, impidiendo el acceso hasta que se abona un rescate.

- Denegación de servicios (DoS): Se basan en la saturación de servidores o infraestructuras con un volumen anómalo de solicitudes, con el objetivo de impedir el acceso legítimo de los usuarios.

- Ataques basados en la web. Son URL maliciosas o scripts maliciosos que se utilizan para dirigir al usuario al sitio web deseado o descargando contenido malicioso.

- Campañas de phishing y otras formas de ingeniería social: Los correos electrónicos fraudulentos siguen siendo uno de los métodos preferidos de los atacantes para obtener credenciales o inducir a los empleados públicos a ejecutar acciones que comprometen la seguridad.

La frecuencia con la que las administraciones locales sufren estos incidentes es muy alta, existiendo numerosos ejemplos de todas las categorías señaladas, a pesar de que en la mayoría de los casos los incidentes no llegan a la opinión pública. Así, es posible recordar episodios de ransomware, como los que paralizaron durante semanas al Ayuntamiento de Sevilla en 2023 y al de Calvià (Mallorca) en 2024, o el pago de un rescate en criptomonedas por parte del Ayuntamiento de Cangas de Morrazo (Pontevedra) en 2023, que está siendo investigado penalmente como posible delito de malversación. También se han producido ataques de denegación de servicio (DDoS), como el que afectó a la Diputación de Gipuzkoa y a varios ayuntamientos guipuzcoanos en marzo de 2025, o el que dejó inaccesible la web del Ayuntamiento de Toledo ese mismo mes. En el ámbito de los ataques basados en la web, son frecuentes los incidentes de defacement y explotación de vulnerabilidades en portales municipales, que han obligado a suspender temporalmente servicios electrónicos en distintos ayuntamientos. Finalmente, los intentos de phishing e ingeniería social son una constante en la operativa diaria: varios consistorios han reconocido campañas de correos fraudulentos dirigidas contra su personal, con el objetivo de obtener credenciales de acceso o inducir transferencias indebidas, lo que demuestra que en los entornos locales estas técnicas constituyen una amenaza persistente. Algunos de estos incidentes tienen como consecuencia el menoscabo de fondos públicos de importes muy elevados, como ocurrió con el desvío de nóminas de los Ayuntamientos de Ro-

1 Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, «El papel de la Administración electrónica en el futuro de Europa» (SEC [2003] 1038).

quetas de Mar y Granada, la estafa *man in the middle* sufrida por el Ayuntamiento de Sevilla o el fraude del CEO en la Empresa Municipal de Transportes de Valencia.

Conscientes de la importancia de evaluar los controles de seguridad de la información, los Órganos de Control Externo aprobaron en 2018 la GPF–OCEX 5313 *Revisión de los controles básicos de ciberseguridad* (CBCS), con el propósito declarado de permitir formar una idea general de la situación en la entidad revisada sin requerir la dedicación de excesivos recursos especializados. Esta guía se elaboró de forma completamente alineada con los requerimientos del ENS, pero reduciendo a ocho los controles a evaluar. Como se menciona en la propia guía, se estima que solo con el adecuado funcionamiento de los seis primeros controles (CBCS 1 a 6), es posible repeler el 85% de los ataques informáticos.

La metodología de la GPF–OCEX 5313 presenta, además, la virtud de ofrecer resultados cuantitativos, evaluando la existencia de los controles en índices de madurez (0-100%), de modo que permite la comparación entre administraciones, el seguimiento de la evolución en una misma entidad a lo largo del tiempo, y la medición de la distancia existente entre la situación actual y el nivel mínimo exigido normativamente.

Hasta la fecha han sido cuatro los OCEX que han iniciado la revisión de los CBCS en entidades locales: la Sindicatura de Cuentas de la Comunidad Valenciana, el Consejo de Cuentas de Castilla y León, el Consejo de Cuentas de Galicia y la Sindicatura de Cuentas de Cataluña, que han evaluado un total de 7 diputaciones, 35 ayuntamientos y una empresa pública municipal, realizándose en algunos casos informes de seguimiento sobre la misma entidad. El conjunto de informes emitidos por los OCEX sobre los CBCS permite observar un nivel realmente bajo en el cumplimiento de las obligaciones impuestas por el ENS. De todas las entidades analizadas, únicamente la Diputación de A Coruña cumplía inicialmente con los niveles de madurez mínimos exigidos por el ENS, y en los informes de seguimiento realizados solo el Ayuntamiento de Benidorm pudo mejorar lo suficiente para alcanzar esos niveles mínimos obligatorios.

2. El enfoque de riesgos en la auditoría de cuentas y el papel de las tecnologías de la información.

El modelo de auditoría contemporáneo, tanto en el sector privado como en el público, pivota sobre un enfoque basado en riesgos, según el cual el auditor centra sus esfuerzos en aquellas áreas donde es más probable que se produzcan errores significativos, irregularidades o incumplimientos. Se trata de una metodología de trabajo que parte de un conocimiento profundo de la organización, de su entorno y de sus procesos clave, para identificar dónde se concentran las mayores vulnerabilidades. A partir de esa valoración, la auditoría se planifica de forma selectiva, dirigiendo más recursos y pruebas hacia los ámbitos de mayor exposición, y reduciendo la intensidad de revisión en aquellos otros con un riesgo bajo. Este enfoque busca optimizar la eficiencia del trabajo, aumentar la probabilidad de detectar errores significativos y, al mismo tiempo, ofrecer conclusiones más útiles para la gestión.

En entidades con uso intensivo de tecnologías de la información, como son las entidades locales actuales, ese conocimiento y evaluación del control interno de la entidad que debe hacer el auditor implicará evaluar las medidas de seguridad informática aplicadas por la entidad, al menos respecto a los tipos de transacciones, saldos contables o información a revelar significativos.

En la valoración de riesgos, la NIA–ES 315 revisada y su transposición en la GPF–OCEX 1315 revisada obligan al auditor a obtener un conocimiento suficiente de la entidad y de su entorno, incluyendo su modelo de negocio y la forma en que este se apoya en las tecnologías de la información. Este conocimiento resulta esencial para identificar los riesgos derivados del uso de las TI, aunque no todos ellos se materializan en riesgos de incorrección significativa en las cuentas anuales. En particular, los riesgos de ciberseguridad son inherentes a cualquier organización, pero su impacto contable dependerá del grado de digitalización de la entidad y de la criticidad de sus sistemas de información en la gestión económico–financiera.

3. Responsabilidades de las intervenciones locales respecto a los controles de ciberseguridad.

Dentro de las funciones tradicionales de los interventores locales resultaría, en principio, impensable extender su ámbito de actuación hasta abarcar controles técnicos sobre las tecnologías de la información, pues la función interventora se ha configurado históricamente en torno a la fiscalización de la legalidad, la regularidad contable y la verificación del destino correcto de los recursos públicos, y en cualquier caso sería el correspondiente departamento informático de la entidad, dotados de personal especializado en la gestión y protección de los sistemas tecnológicos, los llamados a diseñar, implantar y mantener los controles técnicos necesarios en materia de seguridad de la información.

Sin embargo, como hemos visto, la evaluación del riesgo

derivado del uso de tecnologías de la información en la entidad, y de los controles establecidos para mitigarlos, serán etapas imprescindibles en la realización de una auditoría de cuentas de acuerdo con las Normas Internacionales de Auditoría, o sus correspondientes adaptaciones al sector público, siendo este el primer motivo por el que una intervención local debería realizar esta función.

De conformidad con el art. 29.3 del RD 424/2017, la intervención local realizará anualmente la auditoría de las cuentas anuales de:

a) Los organismos autónomos locales.

b) Las entidades públicas empresariales locales.

c) Las fundaciones del sector público local obligadas a auditarse por su normativa específica.

d) Consorcios adscritos a la entidad.

e) Las sociedades mercantiles y las fundaciones del sector público local no sometidas a la obligación de auditarse que se hubieran incluido en el plan anual de auditorías.

Por ello en estas entidades, y con motivo de la realización de la auditoría de cuentas, la intervención local debe evaluar los controles de seguridad informática establecidos en la entidad, al menos los relacionados con los tipos de transacciones, saldos contables e información a revelar considerados significativos en las cuentas anuales.

¿Y en la entidad principal? Respecto a la entidad principal (Ayuntamiento o Diputación), la intervención local no realiza auditoría de cuentas ya que, de hecho, es la encargada de la confección de sus cuentas anuales. Sin embargo, la entidad principal se encuentra sometida al control permanente, y de acuerdo con el art. 32 del RD 424/2017, las actuaciones de control permanente podrán incluir entre otras, la revisión de los sistemas informáticos de gestión que sean precisos.

Por otra parte, existen otras disposiciones que otorgan de manera directa las intervenciones locales responsabilidades sobre el sistema informático de la entidad y su seguridad.

De conformidad con el art. 4.2 del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional, la función de contabilidad incluye, entre otras:

- Coordinar las funciones o actividades contables de la Entidad Local, emitiendo las instrucciones técnicas oportunas e inspeccionando su aplicación.
- Organizar un adecuado sistema de archivo y conservación de toda la documentación e información contable que permita poner a disposición de los órganos de control los justificantes, documentos, cuentas o registros del sistema de información contable por ellos solicitados en los plazos requeridos.
- Inspeccionar la contabilidad de los organismos autónomos, de las sociedades mercantiles dependientes de la Entidad Local, así como de sus entidades públicas empresariales, de acuerdo con los procedimientos que establezca el Pleno.

En adición, de forma general el art. 6 del RD 424/2017, referido a las facultades del órgano de control interno local, incluye entre las mismas las siguientes:

> *"1. El órgano interventor podrá hacer uso en el ejercicio de sus funciones de control del deber de colaboración, de la facultad de solicitar asesoramiento, de la defensa jurídica y de la facultad de revisión de los sistemas informáticos de gestión de acuerdo con lo previsto en los párrafos siguientes*
> *[…]*
> *7. Los funcionarios actuantes en el control financiero podrán revisar los sistemas informáticos de gestión que sean precisos para llevar a cabo sus funciones de control."*

Más claro y con relación directa a los controles de ciber-

seguridad es la facultad establecida en el art. 33.4 de verificar la seguridad y fiabilidad de los sistemas informáticos que soportan la información económico–financiera y contable.

Por todo ello, tanto para la entidad principal como para las entidades dependientes, el órgano interventor tiene entre sus responsabilidades (y facultades), la de verificar la existencia y el funcionamiento de los correspondientes controles de seguridad de la información, al menos los relacionados con el software que directa, o indirectamente tenga repercusión en la información contable de la entidad, entre la que podemos incluir el propio software de contabilidad, pero también el software de administración electrónica, el de gestión de personal y confección de nóminas, o el de gestión de ingresos y recaudación, por ejemplo.

4. Los controles básicos de ciberseguridad.

La GPF–OCEX 5313 en el Anexo 1 describe los ocho controles básicos de ciberseguridad y explica por qué son importantes para la evaluación de la seguridad informática de la organización, y en el Anexo 3, en las fichas de revisión para la realización del trabajo, recoge los subcontroles en los que se desglosan cada uno de ellos, y las pruebas a realizar y posibles evidencias a obtener.

Los ocho controles básicos de ciberseguridad son los siguientes:

CBCS 1. Inventario y control de dispositivos físicos

Este control implica disponer de un inventario completo y actualizado de todos los equipos (servidores, ordenadores, móviles, impresoras, dispositivos de red, etc.) y garantizar que no accedan a la red dispositivos no autorizados. La finalidad es doble: conocer con precisión qué activos deben protegerse y evitar que equipos no controlados introduzcan vulnerabilidades. Para ello se combinan herramientas de descubrimiento automático o registros manuales junto con medidas que bloqueen accesos indebidos. Su importancia radica en que cualquier equipo externo sin control puede convertirse en un punto de entrada de malware y comprometer la seguridad global.

CBCS 2. Inventario y control de software autorizado

Consiste en mantener un catálogo de programas aprobados, revisar periódicamente las aplicaciones instaladas y restringir la ejecución de software no permitido. El uso de programas sin autorización constituye una de las vías más habituales de infección. Este control pretende que solo se ejecute software seguro, evitando versiones obsoletas o maliciosas. Para ello, resulta clave disponer de un inventario actualizado, de una "lista blanca" de aplicaciones permitidas y de un proceso de revisión constante. Aunque limita la libertad de instalación por parte de los usuarios, es una de las medidas más efectivas contra los ciberataques.

CBCS 3. Identificación y corrección de vulnerabilidades

Se trata de localizar de forma continua las debilidades técnicas de los sistemas, valorarlas según su criticidad y aplicar correcciones en plazos razonables. El control exige realizar escaneos periódicos, analizar alertas de seguridad, gestionar parches y documentar las medidas adoptadas. La finalidad es reducir el tiempo en que un sistema permanece expuesto. El uso de herramientas automáticas de detección y gestión resulta esencial para anticiparse a los atacantes, que suelen aprovechar cualquier demora en la aplicación de parches.

CBCS 4. Uso controlado de privilegios administrativos

Busca asegurar que los permisos de administración solo se concedan cuando son estrictamente necesarios y siempre a usuarios identificados. La apropiación indebida de credenciales privilegiadas es una de las técnicas más frecuentes en ciberataques. Este control requiere políticas de privilegios mínimos, revisión periódica de cuentas, contraseñas robustas, autenticación multifactor y supervisión de accesos. Si los permisos se conceden de forma indiscriminada, el riesgo de accesos indebidos y propagación de ataques se incrementa notablemente.

CBCS 5. Configuraciones seguras de hardware y software

Consiste en aplicar configuraciones reforzadas a todos los sistemas, deshabilitando servicios innecesarios, eliminando cuentas por defecto y siguiendo las guías de seguridad de fabricantes y organismos especializados. Muchos equipos se entregan configurados para la facilidad de uso, no para la seguridad. El bastionado inicial debe mantenerse actualizado mediante procedimientos de gestión de cambios, evitando que servicios obsoletos o protocolos inseguros se conviertan en puntos de entrada.

CBCS 6. Registro y análisis de la actividad de los usuarios

La conservación y revisión de logs es básica para detectar y reconstruir incidentes. Este control revisa si la entidad tiene políticas claras de logging, define qué eventos registrar, cómo protegerlos y cuánto tiempo conservarlos. Una buena práctica es centralizar los

registros mediante sistemas SIEM que correlacionan grandes volúmenes de datos y facilitan la identificación de patrones sospechosos. Sin registros completos y revisados, los ataques pueden permanecer ocultos durante largos periodos.

CBCS 7. Copias de seguridad de datos y sistemas
Garantiza la recuperación de la información y la continuidad del servicio tras incidentes graves. Incluye la realización periódica de copias completas, su almacenamiento en distintos soportes y ubicaciones, el cifrado de la información y la existencia de procedimientos de restauración probados. La copia de seguridad solo es eficaz si se acompaña de ensayos regulares de recuperación, que verifiquen la integridad de los datos y la rapidez de respuesta.

CBCS 8. Cumplimiento de legalidad
Este último control evalúa el cumplimiento de diversas normas relacionadas con la seguridad de la información, e indirectamente evalúa la gobernanza de la ciberseguridad, al evaluar el cumplimiento del ENS, que incluye cuestiones tales como la aprobación y difusión de la Política de Seguridad de la Información (PSI), la constitución de un comité de seguridad, la definición de responsabilidades, o la formación y concienciación. Además del cumplimiento de la ENS se evalúa la conformidad con la normativa de protección de datos y las normas de facturación electrónica.

La relevancia de este control es doble: garantiza la legalidad y crea un marco organizativo estable que trasciende lo técnico. Sin una gobernanza clara y procedimientos formalmente aprobados, las medidas de seguridad corren el riesgo de ser parciales, inconsistentes o meramente formales, lo que compromete la eficacia global del sistema de protección.

5. Metodología recogida en la GPF-OCEX 5313. Revisión de los controles básicos de ciberseguridad.

La evaluación se realiza partiendo de la información obtenida de los siguientes medios: mediante entrevistas, inspección documental, observación de procesos y revisión de evidencia técnica. La alineación con el ENS hace que sea posible partir del resultado obtenido en la última auditoría del ENS, de obligatoria realización cada dos años, lo cual simplifica mucho el trabajo a realizar. Por otra parte, la guía recoge en su Anexo 2 un cuestionario que deberá rellenar el responsable del sistema informático de la entidad y que recoge todos los aspectos a evaluar. La flexibilidad del modelo facilita su aplicación en entidades de diferentes tamaños y complejidad y permite establecer objetivos de evolución realistas. El resultado de esta evaluación se traduce en los llamados niveles de madurez, índices de madurez, e índices de cumplimiento.

Niveles de madurez

El ENS, aprobado por Real Decreto 311/2022, establece que la seguridad de los sistemas de información debe evaluarse no solo en términos de medidas técnicas implantadas, sino también de su grado de formalización y eficacia. Para ello se define un esquema de niveles de madurez que clasifica los controles en cinco estadios, además de un Nivel 0 o inexistente:

- Nivel 1 (N1 – Inicial/ad hoc): el control existe de manera incipiente o no está formalizado; depende de iniciativas individuales. Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.
  Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

- Nivel 2 (N2 – Repetible pero intuitivo): el control se aplica de manera reiterada, pero sin procedimientos formalmente aprobados. En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad. Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

- Nivel 3 (N3 – Definido): el control está documentado y formalizado, se aplica de forma homogénea. Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados. Los procedimientos se comunican con acciones formativas.

- Nivel 4 (N4 – Gestionado y medido): el control se supervisa, se mide y se somete a revisiones periódicas. Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad. La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere.

- Nivel 5 (N5 – Optimizado): el control se encuentra en mejora continua, con procesos sistemáticos de retroalimentación. La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Índices de madurez

El índice de madurez es un indicador cuantitativo que refleja el grado de desarrollo de un control de ciberseguridad en una entidad, y de la entidad en su conjunto. Se expresa en forma de porcentaje en una escala del 0-100% tanto para cada control como de forma global. Al igual que los niveles de madurez, los indicadores reflejan el grado de implantación de las medidas de seguridad de la información en una organización, pero la expresión en forma de índice numérico aporta ventajas significativas. En lugar de limitarse a cinco niveles discretos, la escala de 0 a 100 % permite una medición más precisa del grado de cumplimiento y, además, facilita la comparación tanto entre distintas entidades como en la evolución de una misma entidad a lo largo del tiempo.

En la GPF–OCEX 5330 a la que se remite la GPF–OCEX 5313, se recoge la equivalencia entre los niveles e índices de madurez, siendo la siguiente:

- 0–9 % → N0 Inexistente
- 10–49 % → N1 Inicial/ad hoc
- 50-79 % → N2 Repetible pero intuitivo
- 80-89 % → N3 Proceso definido
- 0–99 % → N4 Gestionado y medido
- 100 % → N5 Optimizado

Índice de cumplimiento

Por último, en los informes de evaluación de los CBCS se recoge un índice de cumplimiento, global y para cada control, que resultará de comparar el indicador de madurez con el nivel requerido u objetivo mínimo que tiene el sistema según el ENS.

De acuerdo con la metodología establecida en las GPF–OCEX 5313 y 5330, en primer lugar cada uno de los subcontroles o controles detallados en los que se desglosan los CBCS han de ponderarse en función de la importancia o peso relativo que se le otorgue a cada uno de ellos para la efectividad del control. A continuación han de calificarse en las siguientes categorías: control efectivo, control bastante efectivo, control poco efectivo, control no efectivo o no implantado, y se le ha de asignar un índice de madurez. Para evaluar el índice de madurez de cada control se tienen en cuenta los resultados obtenidos en la revisión de los controles detallados que lo forman y considerando la ponderación o importancia relativa que se les asigna para el cumplimiento del objetivo de control. El índice resultante marcará a su vez el nivel de madurez (N0–N5) conforme a la equivalencia anteriormente reproducida.

Una vez obtenida la evaluación de cada uno de los CBCS, el índice de madurez global de la entidad se calcula mediante la media de los índices de madurez de los controles.

El nivel mínimo exigible de madurez en los controles depende de la categoría ENS del sistema de información evaluado. El ENS distingue tres categorías (baja, media y alta) en función del impacto que tendría una pérdida de seguridad en las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

En los informes de los OCEX sobre entidades locales, todos los sistemas revisados se han calificado como de categoría media. Ello implica que el nivel de madurez objetivo es N3 (definido), equivalente a un índice de madurez mínimo del 80 % en todos los CBCS, que implica que los controles deben estar formalmente establecidos, documentados y aplicados de forma homogénea en toda la organización.

La metodología expuesta hace posible que las intervenciones locales evalúen formalmente la situación de los controles de seguridad de la información de la entidad sin la necesidad de asistencia técnica externa, partiendo simplemente de la información obtenida del cuestionario anexo a la guía o bien de la última auditoría de seguridad del ENS.

Conclusiones.

1. La generalización de medios informáticos y de la administración electrónica en el funcionamiento de las entidades locales incrementa de forma exponencial los riesgos derivados del uso de las tecnologías de la información.

2. El panorama de ciberamenazas (malware, ransomware, DoS/DDoS, ataques web y phishing/ingeniería social) afecta de manera continuada a las administraciones locales, con impactos operativos y patrimoniales que pueden comprometer la continuidad del servicio y la fiabilidad de la información económico–financiera.

3. Desde un enfoque de auditoría basada en riesgos, la evaluación del control interno en entornos intensivos en TI exige revisar, al menos, los controles que inciden en los procesos y aplicaciones con efecto contable o presupuestario (contabilidad, nóminas, recaudación, administración electrónica, etc.).

4. El marco jurídico del control interno local (RD 424/2017) y el estatuto de los habilitados nacionales (RD 128/2018) habilitan y, en la práctica, obligan a la Intervención a verificar la seguridad y fiabilidad de los sistemas que soportan la información económico-financiera. No es una invasión del ámbito técnico: es el ejercicio debido de la función de control.

5. Asimismo, el simple hecho de que la Intervención local emita un informe sobre estos controles puede actuar como un catalizador de mejora, al atraer la atención de los órganos gestores hacia cuestiones que, en circunstancias ordinarias, suelen recibir escasa consideración por parte de la dirección política de la entidad, como podemos observar que ha ocurrido en las entidades locales que han sido objeto de informes de CBCS por parte de los OCEX.

6. La GPF–OCEX 5313 (CBCS) constituye un instrumento idóneo, proporcionado y operativo para cumplir esa responsabilidad: está alineado con el ENS, focaliza en ocho controles de alto impacto, y traduce la revisión a índices de madurez comparables y trazables en el tiempo.

BIBLIOGRAFÍA

- Benítez Palma, E., & Vaz Calderón, C. (2019). La ciberseguridad en las entidades locales: cómo enfocar una fiscalización externa de cumplimiento de legalidad. Auditoría pública nº74.
- Olano Salvador, M. (2024). La importancia de los controles de ciberseguridad en las fiscalizaciones de los ICEX. Auditoría Pública nº83 junio 2024, 95-104.
- Guía práctica de fiscalización GPF–OCEX 5313. Revisión de los controles básicos de ciberseguridad.
- Guía práctica de fiscalización GPF–OCEX 5330. Revisión de la ciberseguridad en las entidades públicas.