Guía práctica de fiscalización de los OCEX

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

Referencia: GPF-OCEX 1315, 1500 y 5300

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 27/11/2017

1. Introducción

En los últimos años se ha acentuado el fenómeno de la generalización y creciente dependencia de las tecnologías de la información y las comunicaciones (TIC) en el desarrollo de las actividades de las administraciones públicas, tanto en sus relaciones con ciudadanos y proveedores, como en su gestión interna. Este hecho ha originado que hayamos asistido a un crecimiento sin precedentes de ataques de muy distinto tipo, procedencia y objetivos a los sistemas de información públicos y a los datos en ellos procesados y almacenados.

En un mundo interconectado en el que las distintas redes de las administraciones públicas no son sino elementos integrantes de una red global, los ciberriesgos se multiplican.

Viendo la amplitud de las amenazas (agentes de las amenazas más significativos durante 2016, la tipología de sus acciones y sus víctimas) señaladas en el informe del Centro Criptológico Nacional (CCN) "Ciberamenazas y Tendencias 2017" que se muestran en el Anexo 1, o revisando la taxonomía de amenazas de ciberseguridad publicada por ENISA que se muestra en el Anexo 2, se llega a la conclusión de que la ciberseguridad es una materia muy importante, que debe ser abordada por todas las entidades públicas de forma integrada con sus políticas de seguridad de la información en su sistema de control interno.

Actualmente la ciberseguridad se ha convertido en uno de los temas más relevantes tanto para los gobiernos, como para los gestores públicos, y por supuesto para los auditores públicos, dada la potencial repercusión que las amenazas a la seguridad de los sistemas de información representan no solo sobre las cuentas que se auditan si no a la misma continuidad en la prestación de servicios públicos. El auditor público también debe tener en consideración las diversas normas legales que establecen obligaciones en esta materia y cuyo cumplimiento tiene una importancia paralela a la de los controles que se establecen en ellas.

El objetivo de la presente guía es servir de introducción a la problemática que la ciberseguridad plantea en la actividad de los auditores de los OCEX, concienciar sobre su importancia y señalar algunas líneas de desarrollo posterior de las GPF-OCEX.

2. La ciberseguridad y la seguridad de la información

La Directiva 2016/1148 de Ciberseguridad define la *seguridad de las redes y sistemas de información* (es decir la ciberseguridad) como la *capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la* ***disponibilidad***, ***autenticidad***, ***integridad*** *o* ***confidencialidad*** *de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos*.

Esta definición es coincidente con la del Esquema Nacional de Seguridad y contempla las **características fundamentales de la información** que la ciberseguridad debe garantizar. Junto con la trazabilidad forman las cinco dimensiones[1] de seguridad:

- La **disponibilidad** trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
- La **confidencialidad** es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
- La **integridad** es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
- La **autenticidad** es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- La **trazabilidad** es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Los conceptos de seguridad de la información y ciberseguridad se utilizan frecuentemente de forma indistinta, pero existen unos matices que los diferencian. La seguridad de la información trata de la protección de la información dentro de una entidad, independientemente de su formato. La ciberseguridad se ocupa específicamente de la protección de los activos de información procesada, almacenada y transportada por **redes y sistemas de información interconectados**.

Un ejemplo ayudará a entender la diferencia. En una entidad pequeña, que disponga de un servidor para gestionar su contabilidad, nóminas, compras, etc, con una red interna que no esté conectada a internet, consideraremos en la auditoría la problemática de la seguridad de la información, los CGTI y los controles de aplicación. Pero no habrá problemática relacionada con la ciberseguridad.

En una entidad de gran tamaño, con servicios a los ciudadanos por internet, con una administración electrónica desarrollada, con múltiples ubicaciones geográficas interconectadas, con servicios web que conectan con los

---

[1] La publicación del Centro Criptológico Nacional y de la Federación Española de Municipios y Provincias, "Guía estratégica en seguridad para entidades locales" de octubre de 2017, intenta aclarar este concepto:

"…en realidad, ¿qué significa cada una de estas dimensiones? Veamos algunos ejemplos:

- La **disponibilidad** actúa sobre la no interrupción del servicio (p.ej. La Web corporativa, perfil de contratante o algunos trámites electrónicos en la sede dejan de funcionar y no están accesible a través de internet.)
- La **autenticidad** protege el aseguramiento de la identidad (p.ej. La identidad de la persona que ha firmado un documento, quién se ha conectado a través de una red WIFI, etc.)
- La **confidencialidad** previene la filtración de información (p.ej. Gestionar el acceso a determinado tipo de información.)
- La **integridad** previene manipulaciones de la información (p.ej. Disponer de documentos que han sido firmados de forma electrónica, asegurar la fecha de publicación de un documento en la sede electrónica, etc.)
- La **trazabilidad** permite conocer posibles rastros en accesos (p.ej. sistema de registro de accesos por parte de usuario, análisis de posibles fugas de datos, intrusión a sistemas de ataques externos, etc.)"

La literatura internacional sobre la materia, en general, habla de tres dimensiones o características fundamentales de la seguridad: confidencialidad, integridad y disponibilidad. El *WGITA-IDI Handbook on IT Audit for SAI* también, y señala que la integridad está formada por la autenticidad y el no repudio. En definitiva las cinco dimensiones del ENS solo son una extensión de las tres fundamentales.

proveedores, etc, la problemática de la ciberseguridad será un área de riesgo y de especial consideración en la auditoría.

El gran crecimiento de las **redes y sistemas de información interconectados** es lo que ha originado que dentro del dominio de la seguridad de la información se haya producido un creciente auge de los temas relacionados con la ciberseguridad. Actualmente las amenazas a la seguridad de los activos de información provienen de un variado y creciente número de fuentes, muchas de ellas a través de internet.

En todo caso, las políticas y controles de ciberseguridad deben estar alineados con las políticas de seguridad de la información de las organizaciones públicas y, por su trascendencia e impacto, el auditor público debe incluir en su metodología ordinaria de trabajo la revisión de los controles de seguridad de la información, incluyendo la ciberseguridad.

En síntesis podemos decir que **la finalidad de la ciberseguridad es proteger los activos[2] de información procesada, almacenada y transportada por redes y sistemas de información interconectados**.

3. Propiedades o características de la información digital y de la evidencia electrónica

Acaba de señalarse que la información y los datos que circulan, almacenan o se procesan en un sistema de información deben tener una serie de características que los controles de seguridad deben garantizar, tal como requiere la Directiva de Ciberseguridad a nivel europeo.

También, de acuerdo con lo previsto en el Esquema Nacional de Seguridad los datos, informaciones y servicios utilizados en medios electrónicos por las Administraciones Públicas, deberán contar con medidas de seguridad que garanticen su acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación.

En el marco de una fiscalización, dichas características son esenciales para que la información y los datos obtenidos en formato digital por los auditores de los sistemas de información del ente auditado puedan considerarse evidencia fiable. Con esta finalidad **los auditores externos deben revisar los controles internos diseñados e implantados en los sistemas de información para garantizar que los datos utilizados como fuente de evidencia tienen esas características**.

De acuerdo con la GPF-OCEX 1500 (apartado 37), los criterios, propiedades o características que permitirán valorar la fiabilidad de la información y garantizar la misma como evidencia de fiscalización en los entornos informatizados son los siguientes:

Autenticación:	Se refiere a la posibilidad de confirmar, de forma indubitada, la identidad de la persona o entidad que creó, originó o de la que procede la información *(Autenticidad)*.
Autorización:	Se refiere al hecho de que la información electrónica ha sido creada, procesada, grabada, corregida, enviada, archivada, ingresada y destruida solo por personas autorizadas y responsables.
Confidencialidad:	La información únicamente será conocida por las personas o entidades autorizadas (quienes la originan y a quienes va dirigida).
Integridad:	Es la garantía de que los datos o información de origen han sido validados y estos no han sido alterados al ser creados, procesados, transmitidos y almacenados en los sistemas informáticos.
Disponibilidad:	La información ha de estar disponible para las personas o entidades autorizadas, evitándose las pérdidas de datos.
Trazabilidad:	Indica las acciones o procesos que se llevan a cabo en el sistema, así como quién y cuándo las realiza.
No repudio:	Imposibilidad de que una persona o entidad que haya originado, transmitido o recibido información pueda negar haber participado en ese origen o intercambio de datos. (*Según INCIBE, el no repudio puede considerarse sinónimo de autenticidad*).

[2] Se entiende por activo cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Esta exigencia de la GPF-OCEX 1500 está respaldada por lo previsto en los artículos 17 de la Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas y 46 de la Ley 40/2015, Régimen Jurídico del Sector Público que establecen que los documentos administrativos se almacenarán por medios electrónicos y deberán conservarse en un formato que permita garantizar su autenticidad, integridad, conservación, disponibilidad y accesibilidad.

Vemos que las propiedades que el auditor debe exigir a la evidencia digital son básicamente coincidentes con las características de la información que el Esquema Nacional de Seguridad (en adelante, ENS) pretende garantizar.

Por tanto una entidad que acredite el cumplimiento con el ENS, fundamentalmente mediante las auditorías de seguridad previstas en su artículo 34, proporcionará a los auditores de los OCEX una seguridad más elevada que la que proporcione una entidad que no acredite su conformidad con el ENS.

En estos últimos casos **los auditores deberán realizar procedimientos adicionales para obtener un determinado nivel de seguridad respecto de la evidencia digital que soporte los informes de fiscalización** (cualquiera que sea el tipo de fiscalización realizada, financiera de legalidad u operativa).

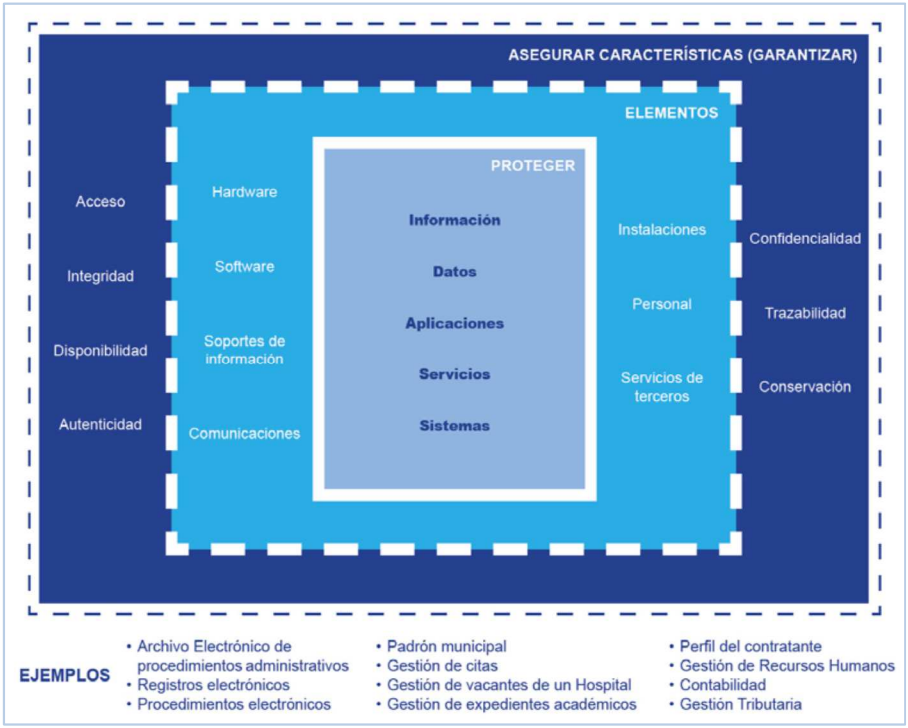
4. Normas sobre seguridad de la información y ciberseguridad

En noviembre de 2016 entraron en vigor en nuestro país las ya citadas leyes 39/2015, y la 40/2015. Estas leyes constituyen el eje vertebrador de las relaciones de los ciudadanos y sus Administraciones Públicas y de estas entre sí, consagrándose el uso de las herramientas electrónicas, basadas en sistemas de información interconectados, como el medio habitual para encauzar tales relaciones y el principio de "**digital por defecto**" en el funcionamiento de la Administración.

Según la Ley 40/2015, el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El ENS, regulado en el Real Decreto 3/2010, de 8 de enero y actualizado por el Real Decreto 951/2015, de 23 de octubre, es el elemento normativo que pretende garantizar la adecuada protección de la información tratada y los servicios prestados por las entidades del sector público.

El ámbito de aplicación objetivo o material del ENS puede representarse en el gráfico siguiente:



Fuente: Guía de seguridad (CCN-STIC-830) Ámbito de aplicación del ENS

La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios

electrónicos. Señala que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

En el artículo 34 del ENS se establece que todas las entidades públicas están obligadas a cumplir con el ENS y someter sus sistemas de información a una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de sus requerimientos. También se deberá realizar una auditoría con carácter extraordinario "siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior."

El objetivo final de esta auditoría de seguridad, realizada por expertos, es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado, tanto internamente como frente a terceros, que pudieran estar relacionados; es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

El artículo 41 del ENS señala que: "Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad."

Según la categoría del sistema se distingue entre:

- **Declaración de Conformidad**: de aplicación a sistemas de información de categoría **Básica**. Podrá representarse mediante Sello o Distintivo de Declaración de Conformidad generado por la entidad bajo cuya responsabilidad esté el sistema.
- **Certificación de Conformidad**: de aplicación obligatoria a sistemas de información de categoría **Media** o **Alta** y voluntaria en el caso de sistemas de información de categoría Básica. Sus símbolos acreditativos son:

La progresiva implantación de la Administración Electrónica hace que, además de la estricta obligación legal de implantar el ENS, los OCEX deban considerar el riesgo, grande y creciente, que las cuestiones relacionadas con la ciberseguridad tienen en los entes públicos, en las auditorías realizadas sobre ellos, y en la capacidad de reducir dichos riesgos que tiene una adecuada implantación el ENS.

Por esta razón, el ENS adquiere una gran trascendencia y los OCEX deberán verificar en las fiscalizaciones el cumplimiento de la legalidad en relación con el ENS y si no se acredita la adecuación al mismo se deberá reflejar en el informe como un **incumplimiento grave o muy significativo**.

Por otra parte, el 6 de julio de 2016 se aprobó la Directiva 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también conocida como Directiva de Ciberseguridad o Directiva NIS. Actualmente España está en proceso de transponer dicha Directiva, que establece que los estados miembros adoptarán y publicarán, a más tardar el 9 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a la misma.

Otra norma con importante efecto sobre aspectos de la confidencialidad de la información, es el nuevo Reglamento General de Protección de Datos de la UE, aprobado el 27 de abril de 2016 y de plena aplicación para el sector público. Este RGPD será aplicable a partir del 25 de mayo de 2018, fecha a partir de la cual las políticas de seguridad de la información y los controles internos deberán contemplar sus requerimientos.

En un nivel más detallado, el Centro Criptológico Nacional, creado en 2004, que es la entidad que tiene encomendada las funciones relativas a la seguridad de las tecnologías de la información y de protección de la

información clasificada, elabora y difunde normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC de la Administración. Dichas guías son una referencia esencial en la materia.

5. Consecuencias de un incidente de ciberseguridad

Los incidentes de seguridad tienen un coste global, derivado de varios costes parciales: económicos directos, de servicio, de imagen y reputación, por sanciones, etc. Según el CCN los costes más significativos de los ciberincidentes y su gestión son[3]:

- Tiempo de inactividad

  Pérdidas económicas y daños de reputación. En el caso de empresas de servicios públicos, la falta de energía o de agua podría afectar a millones de personas.

  A principios de 2017, el troyano Wannacry provocó el cierre temporal de sistemas enteros de entes públicos y privados. Algunas empresas de transporte público tuvieron que paralizar su actividad. También afectó gravemente al sistema de salud británico[4].

  Vulnerabilidades de ciberseguridad como la conocida en julio de 2017 sobre el servicio LEXNET provocó el cierre temporal de ese servicio esencial para la Administración de Justicia. Además se vulneró la confidencialidad de miles de datos personales de especial protección.

- Costes económicos

  Costes económicos: costes derivados de la respuesta a incidentes, responsabilidad económica frente a sus clientes e, incluso, pago de sanciones por motivos legales.

  Relacionado con el asunto LEXNET, el Consejo de Ministros del 25 de agosto aprobó una inversión de 61 millones de euros para mejoras de los sistemas de información relacionados de la Administración de Justicia.

  La Comisión Europea ha señalado[5] que el fraude con los pagos con tarjetas de crédito asciende al menos a 1.400 millones de euros en la UE.

- Pérdida de datos

  La pérdida de información personal de los clientes o propiedad intelectual, pueden afectar a las finanzas, la marca y la reputación. Los ciberdelincuentes pueden amenazar con publicar datos robados, en un intento de obtener más dinero de la víctima.

  Uno de los sectores que más está en la diana de los ciberdelincuentes es el de los datos personales relativos a la salud, área especialmente sensible y objeto de protección especial.

- Pérdida de vidas

  En el caso de un hospital, la vida de los pacientes puede ponerse en riesgo[6]. Los registros, incluyendo historia clínica, pueden quedar inaccesibles, lo que provocaría retrasos en el tratamiento, la prescripción de medicamentos incorrectos, u otros efectos potencialmente perniciosos.

La interrupción de los servicios prestados al ciudadano en el actual entorno de administración electrónica representa no solo costes para la administración sino para todos los ciudadanos. En estos casos podríamos hablar de Pérdidas de derechos, en todos aquellos procedimientos o asuntos que tengan fecha límite de presentación (ayudas sociales, presentación a oposiciones, contrataciones, etc).

Las estimaciones globales de los costes derivados de las ciberamenazas realizados por diversos analistas ofrecen cifras elevadísimas.

---

3 Ciberamenazas y Tendencias. Edición 2017, CCN-CERT IA-16/17. Resumen ejecutivo.

4 Véase el informe Investigation: WannaCry cyber attack and the NHS, UK NAO, octubre de 2017.

5 State of the Union 2017: The Commission scales up its response to cyber-attacks. 19/09/2017.

6 Véase el informe de la UK NAO.

6. Ciber-resiliencia

La resiliencia es una cualidad inherente a un organismo o entidad, empresa o estado que le permite hacer frente a una crisis sin que su actividad se vea afectada. Así, la ciber-resiliencia es la habilidad para continuar proporcionando servicios al mismo tiempo que se previene, disuade y responde a ciberataques[7]. También reduce la probabilidad de que estos ataques tengan éxito.

Ciber-resiliencia se refiere generalmente a las capacidades organizativas y técnicas para absorber impactos externos e internos, y recuperar la normalidad en las operaciones de una forma controlada.

La Estrategia de Ciberseguridad Nacional aprobada en 2013 incluye la ciber-resiliencia en sus dos primeros objetivos específicos, en particular el primero se refiere a las administraciones públicas de la siguiente forma:[8]

> "Objetivo I Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia."

Se presumirá que una entidad es ciber resiliente cuando tenga implementado un conjunto coherente e integrado de CGTI como el ENS.

7. Consideraciones sobre ciberseguridad en las fiscalizaciones de los OCEX

La ciberseguridad puede ser abordada en una fiscalización de distintas formas, dependiendo del objetivo y alcance de cada fiscalización. Caben dos enfoques principales:

7.1 Auditorias operativas o específicas de ciberseguridad o de sistemas de información

Dependiendo de los objetivos y alcance de la auditoría, pueden plantearse trabajos como:

- Auditorias de los controles de ciberseguridad y de ciberresiliencia.
- Auditoría de seguridad de la información.
- Auditoria de seguridad de los registros contables de facturas electrónicas.
- Auditoría de los sistemas de control interno automatizados.
- Auditoría de los controles de seguridad de la receta electrónica.
- Etc.

Si se realiza una auditoría informática no integrada en una auditoría financiera, generalmente todas las categorías de controles y todos los CGTI pueden ser relevantes excepto que expresamente se excluyan del alcance de la auditoría.

Los objetivos y alcances posibles son numerosos, y tan variados como se establezca en la planificación general del OCEX. Un enfoque posible, podría consistir en revisar el cumplimiento con los 20 Controles Críticos de Seguridad del Center for Internet Security (CIS) que se adjuntan en el anexo 4.

Otro enfoque podría basarse en replicar total o parcialmente las medidas de control previstas en el ENS (ver Anexo 3).

---

7 "Ciber-resiliencia se ha definido partiendo de la definición de resiliencia y restringiendo las posibles fuentes de crisis a eventos tecnológicos y procedentes del ciberespacio, o también se ha definido limitando la dimensión afectada de la empresa a lo que son sus sistemas de proceso de datos y sus comunicaciones. Dada la complejidad de las organizaciones, y la interdependencia entre los distintos elementos que las forman: personal, entorno social, suministros, infraestructura TIC, procesos, ...; no se puede trazar una línea divisoria clara entre lo que supone la resiliencia de la misma y la ciber-resiliencia de sus sistemas. Una y otra están íntimamente relacionadas, es más, son un mismo concepto. No se puede crear una infraestructura tecnológica ciber-resiliente si la organización en sí no es resiliente. La organización es un todo, y el departamento TIC no es un ente independiente que puede sobrevivir o pretender ser inmune a los eventos que pueden sacudir a su personal y sus usuarios." Luis de Salvador Carrasco, en Ciber-resiliencia", Documento Opinión 35/2015, 3/4/2015, en **ieee.es**.

8 La UE también ha manifestado reiteradamente su preocupación por la ciberseguridad y la ciber-resiliencia.

En general una auditoría de ciberseguridad tendrá por finalidad determinar si se garantizan las características fundamentales de la información y el cumplimiento de la normativa. Es decir se verificará que:

- Están implantados los controles adecuados para garantizar la integridad y la fiabilidad de la información almacenada y procesada en los sistemas de información.
- La confidencialidad de los datos sensibles está protegida.
- La disponibilidad de los sistemas de información está asegurada.
- Existen controles que posibilitan una adecuada trazabilidad de las acciones realizadas en los sistemas.
- El cumplimiento de las leyes, reglamentos y estándares aplicables (de especial relevancia en las administraciones públicas).

7.2 Auditorias de seguridad de la información en apoyo de auditorías financieras o de cumplimiento

Los auditores responsables de cada auditoría deben analizar cómo afectan las cuestiones relacionadas con la seguridad informática y la ciberseguridad a los objetivos de su auditoría. Cuanto mayor sea la entidad auditada y más complejos sus sistemas de información, mayor impacto tendrán los aspectos tecnológicos y los riesgos TIC, y mayores serán las consideraciones al respecto que deba hacerse el auditor.

Las GPF-OCEX 1315-1316/NIA-ES 315 requieren que en las auditorías financieras de cuentas anuales o de elementos de las cuentas anuales (por ejemplo: de la cuenta general de un ayuntamiento, de la liquidación del presupuesto, de los gastos de personal, de los ingresos tributarios) el auditor obtenga **un conocimiento suficiente sobre cómo utiliza el ente auditado los sistemas de información, sobre los controles automatizados y su impacto en los estados financieros**. Esto incluye revisar los CGTI (que básicamente están formados por los controles de seguridad de la información y ciberseguridad) con el alcance específico que se determine, en concordancia con el alcance y objetivos de la auditoría.

Solo tras adquirir ese conocimiento se podrán valorar los riesgos de incorrección material en los estados financieros, por ejemplo, los riesgos resultantes de un acceso no autorizado a los sistemas de información y de una utilización y disposición no autorizados de los activos de información de la entidad.

En las auditorías de los sistemas de información en apoyo de una auditoría financiera, los expertos en seguridad TI analizarán con los auditores financieros aquellos controles que son **relevantes para los objetivos de la auditoría financiera**, ya que no todos los riesgos que pretenden mitigar los CGTI son iguales, ni en probabilidad, ni en su materialidad. Para determinar que controles son relevantes se deberá adoptar un enfoque basado en el análisis del riesgo.

Los auditores deben conocer los controles automatizados que tienen impacto en el proceso de elaborar la información financiera incluyendo los controles generales de tecnología de información (CGTI), que están formados principalmente por controles relacionados con la seguridad de la información y la ciberseguridad.

Por ejemplo, si se audita el gasto de la gestión de la receta electrónica, una parte importante del trabajo debería ser abordado por auditores especializados que revisarán los sistemas de información relacionados con la receta electrónica, los CGTI y la ciberseguridad. El caso de la gestión de la receta electrónica es un ejemplo muy claro de la problemática de la ciberseguridad ya que ese proceso está respaldado por un complejo conjunto de aplicaciones y sistemas de información interrelacionados a través de redes públicas y privadas, con múltiples actores, en el que los ciberriesgos son muy elevados. Hoy en día ciberdelincuentes podrían introducir recetas falsas en el sistema sin necesidad de acudir a un médico o una farmacia y cobrar el dinero fraudulentamente obtenido, cómodamente sentados en una ciudad de Asia o de América, suplantando las identidades electrónicas de facultativos y farmacias. Para evitar este tipo de fraude están los controles de ciberseguridad.

Siguiendo con este ejemplo, se puede afirmar que solo el trabajo conjunto e integrado de auditores financieros y de sistemas de un OCEX, permite hoy día fiscalizar este componente muy significativo del gasto sanitario. Como en muchos otros ejemplos que se podrían poner, auditar de otra forma en el siglo XXI no es posible.

El trabajo de los expertos en seguridad de la información, cuando se realiza en apoyo de auditorías financieras o de cumplimiento, debe ser un trabajo más estructurado y estandarizado que el realizado en auditorías ad-hoc comentadas en el apartado anterior, y debe de estar basado en la revisión de los CGTI seleccionados de acuerdo con el enfoque de riesgo y de las necesidades de los auditores financieros, con los que se debe trabajar de forma conjunta e integrada.

8. Ciberseguridad y los CGTI

El área que recoge el trabajo de auditoría de sistemas de información que contempla los riesgos y controles más directamente relacionadas con la ciberseguridad es la relativa a los controles generales de las TI (CGTI).

De acuerdo con la metodología en desarrollo por la Comisión Técnica de los OCEX, basada en las NIA-ES, la revisión de los CGTI se estructura en las cinco categorías siguientes[9]:

A. Marco organizativo

B. Gestión de cambios en aplicaciones y sistemas

C. Operaciones de los sistemas de información

D. Controles de acceso a datos y programas

E. Continuidad del servicio

La guía detallada de fiscalización de los CGTI, incluyendo los controles de seguridad y ciberseguridad, que está elaborando la Comisión Técnica de los OCEX, estará alineada en la mayor medida posible con los controles establecidos en el ENS (véase el Anexo 3), y por extensión con el nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que será de aplicación a partir del 25 de mayo de 2018, de forma que si se acredita la efectiva adecuación al ENS, con la auditoría de seguridad obligatoria por ejemplo, se pueda reducir el alcance de las pruebas de CGTI y ciberseguridad que deba realizar el OCEX, evitando de esta forma molestias al ente fiscalizado y realizando nuestro trabajo con la mayor economía de recursos posible.

9. Selección de los controles relevantes para revisar en una auditoría financiera

Debido al gran número de CGTI que existen en una entidad mediana o grande **resulta materialmente imposible para un auditor revisarlos en su totalidad**. Además, gran parte de ellos no tendrán interés para los objetivos de la auditoria y solo un pequeño subconjunto tendrá impacto sobre el riesgo de auditoria. Es sobre este grupo de controles sobre los que debe centrarse la atención y el trabajo del auditor.

Para seleccionar los controles internos a revisar, incluyendo los de ciberseguridad, el auditor de estados financieros utilizará un enfoque de riesgo, de arriba-abajo en la auditoría del control interno, siguiendo la metodología de la GPF-OCEX 1315. Para cada área o aplicación significativa identificada se requiere que:

a) Se valoren los riesgos de incorrección material relacionados.

b) Se revise la eficacia de los CGTI.

   La importancia de los CGTI es tal, que del resultado de su revisión dependerá la naturaleza, extensión y momento de realización de las pruebas sobre los controles del proceso/aplicación y de las pruebas sustantivas.

c) Se revise la eficacia de los controles del proceso/aplicación.

d) Se realicen las pruebas sustantivas.

Este enfoque permitirá que el auditor se centre solo en los controles que están relacionados con los sistemas y las aplicaciones significativas a efectos de la información contable, financiera o presupuestaria auditada, de acuerdo con los objetivos y alcance de la auditoría que se esté realizando. Es decir, aquellos cuyo buen funcionamiento afecta a las aplicaciones identificadas cómo significativas a los efectos de la fiscalización. El resto carece de interés para la auditoria.

Si se revisan los CGTI de algún sistema o subsistema que no tiene relación con la información contable, financiera o presupuestaria auditada se estará haciendo un trabajo innecesario y por tanto ineficiente.

Por ejemplo, si se está revisando una aplicación de gestión de nóminas por ser los gastos de personal un área significativa, los procedimientos de revisión de los controles generales estarán focalizados en aquellos que afectan más directamente a esa aplicación. En este caso no tendría ningún interés revisar los controles relacionados con el desarrollo y mantenimiento de la aplicación de gestión del inventario de inmovilizado.

[9] Esta estructura, establecida en el apartado 9.2 de la CPF-OCEX 1316, es totalmente coherente con el *Handbook on IT Audit* de INTOSAI.

Tampoco se revisarían los controles de acceso o la gestión de usuarios de la aplicación de ingresos, ya que esos trabajos no nos permitirían reducir el riesgo de auditoría del área de gastos de personal. Se deberían revisar los CGTI relacionados con la aplicación de recursos humanos, con la de nóminas, las bases de datos de ambas aplicaciones, y con los sistemas operativos y servidores que soportan dichas aplicaciones y bases de datos.

Los ciberincidentes normalmente se inician a través de los niveles/capas de la red perimetral e interna, que tienden a estar cada vez más alejados/as de las aplicaciones, bases de datos y sistemas operativos que son los que, habitualmente, se suelen incluir en las pruebas de controles de acceso a los sistemas que afectan los estados financieros. La revisión de determinados controles, como por ejemplo la protección perimetral de la red frente a intrusiones y los accesos a la intranet, la revisión de la configuración de los cortafuegos existentes en los puntos de acceso a las redes corporativas, requiere perfiles técnicos muy especializados en los equipos de auditoría de sistemas de información.

También será importante revisar los controles de acceso lógico (contraseñas, identificación y autenticación de usuarios), la gestión de usuarios de las aplicaciones significativas para la auditoría y de las bases de datos subyacentes, y los cambios en los sistemas que podrían tener efectos en los estados financieros. Una típica prueba de auditoría en esta área que consiste en verificar que los denominados “superusuarios” o usuarios privilegiados están debidamente restringidos al mínimo estrictamente necesario y además que están debidamente controlados.

Si el número de aplicaciones significativas es elevado, tal como sucede por ejemplo en la auditoría de las cuentas de una comunidad autónoma, será imposible revisar en una fiscalización todos los controles de aplicación y CGTI relacionados con todas las aplicaciones significativas. En estos casos se diseñará un plan de rotación del énfasis, es decir, un plan de auditoria plurianual que establezca un calendario para la revisión de forma rotativa de los controles automatizados, tanto de aplicación cómo generales, que sea factible realizar con los recursos del OCEX.

10. Los equipos de auditoría y la ciberseguridad

Para auditar entidades medianas o grandes operando en un entorno de administración electrónica deben formarse **equipos mixtos**, integrados por auditores financieros y por especialistas en auditoría de sistemas de información y ciberseguridad, trabajando conjuntamente con metodología actualizada, de forma que se haga un trabajo adaptado a las nuevas circunstancias mucho más eficaz y eficientemente.

No hacerlo de esta forma, no abordando los riesgos relacionados con la seguridad de la información y la ciberseguridad, supone aceptar unos riesgos de auditoría hasta niveles muy elevados.

Los OCEX deben estar preparados para enfrentar el nuevo entorno y abordar los riesgos relacionados con la ciberseguridad, ya que no solo las actividades ordinarias se realizan a través de sistemas de información interconectados. Las actividades fraudulentas, corruptas y delictivas, también se realizan cada vez más por medios electrónicos aprovechando las vulnerabilidades que los sistemas de información de las administraciones públicas puedan ofrecer.

Hasta que se incorporen a las plantillas de los OCEX auditores de sistemas de información y expertos en ciberseguridad, se dispone del recurso de contratar expertos externos para cubrir ese déficit de conocimientos y de profesionales especializados.

Por otra parte, puesto que cada vez más organizaciones públicas confían en las TIC para automatizar sus operaciones, la línea que separa el rol de los auditores de sistemas de información y el resto de auditores es cada vez más difusa. El auditor financiero es responsable de valorar los riesgos de incorrección material en los estados financieros, incluyendo los derivados de accesos no autorizados a los sistemas de información, por lo que cada vez se va a tener que relacionar más extensamente con el personal de sistemas de los entes fiscalizados y tendrá que considerar personalmente cuestiones relacionadas con la seguridad de la información.

En consecuencia, cada vez más, el perfil del auditor financiero va a requerir un mayor componente tecnológico, aspecto este que deberá incorporarse en los mecanismos de acceso a las plantillas de los OCEX.

El personal actual debe recibir continuas actividades formativas relacionadas con la administración electrónica, la seguridad de la información, la ciberseguridad y las TIC en general.

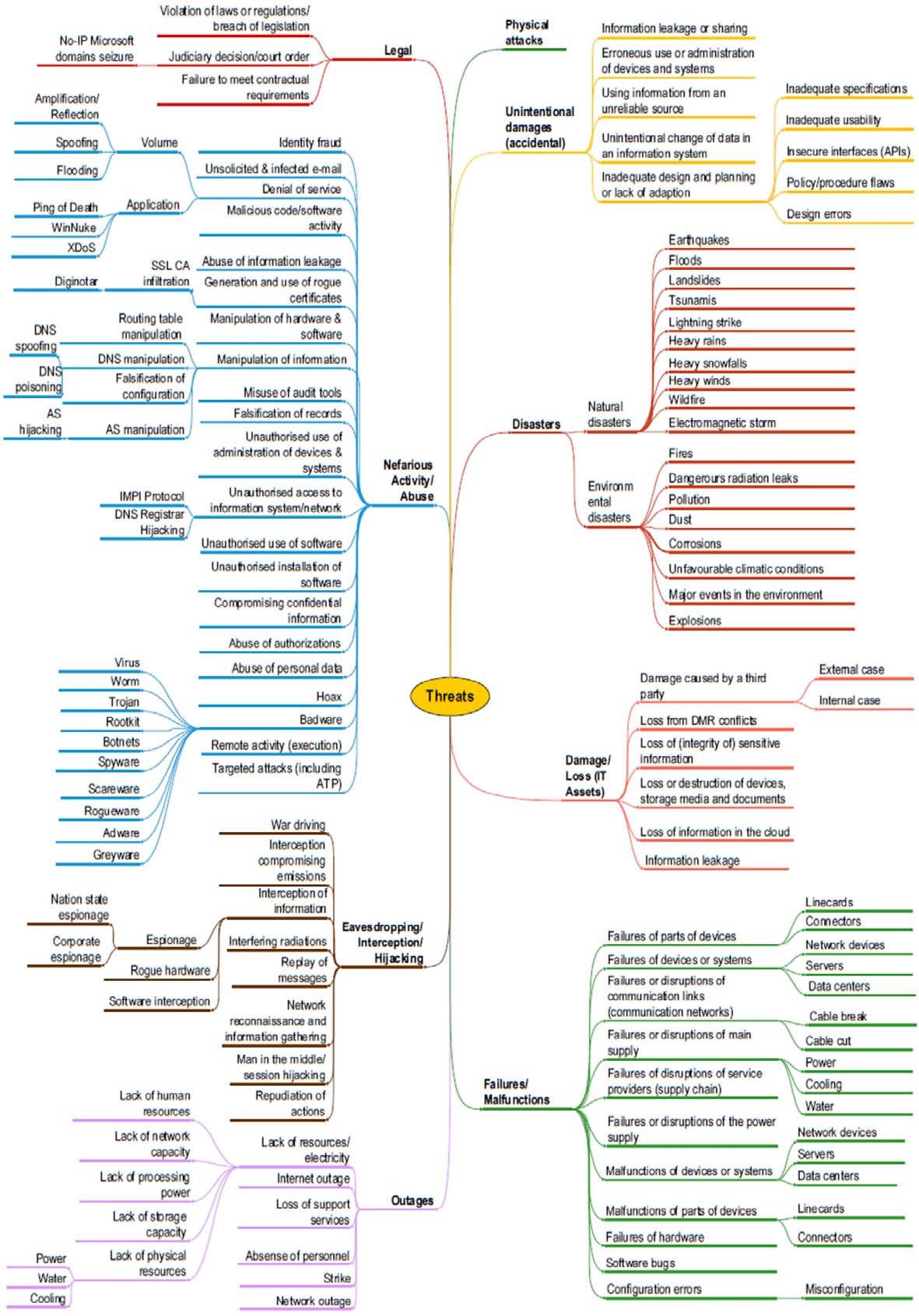
Anexo1 Amenazas más significativas, tipología de sus acciones y sus víctimas[10]

Agentes de las amenazas	Víctimas		
	Sector Público	Organizaciones privadas	Ciudadanos
Estados	Ciberespionaje político	Ciberespionaje económico	Ciberespionaje
	Capacidades ofensivas	Capacidades ofensivas	
Organizaciones criminales	Robo y publicación o venta de información	Robo y publicación o venta de información	Robo y publicación o venta de información
	Manipulación de la información	Manipulación de la información	Manipulación de la información
	Disrupción de sistemas	Disrupción de sistemas	Disrupción de sistemas
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Organizaciones privadas		Ciberespionaje industrial o económico	Abuso o reventa de información corporativa
Ciberterroristas	Disrupción / toma de control de sistemas	Disrupción / toma de control de sistemas	
Ciberyihadistas	Propaganda / Reclutamiento	Propaganda / Reclutamiento	Propaganda / Reclutamiento
Ciberactivismo	Robo y publicación de información	Robo y publicación de información	
	Desfiguraciones	Desfiguraciones	
	Disrupción de sistemas	Disrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	
Ciber vándalos y script kiddies	Robo de información	Robo de información	Robo de información
	Disrupción de sistemas	Disrupción de sistemas	
Actores internos	Robo y publicación o venta de información	Robo y publicación o venta de información	
	Disrupción de sistemas	Disrupción de sistemas	
Ciber-investigadores	Publicación de información	Publicación de información	

Código de colores:	No han aparecido nuevas amenazas. o Existen suficientes medidas para eliminar la amenaza o No han existido incidentes apreciables derivados de la amenaza.	Se han observado nuevas tendencias o fenómenos asociados con la amenaza. o Existe un conjunto de medidas limitadas para eliminar la amenaza o El número de incidentes derivados de la amenaza no ha sido especialmente significativo	Existen claros desarrollos relacionados con la amenaza o Las medidas desplegadas tienen un efecto limitado en la amenaza o El número de incidentes derivados de la amenaza ha sido significativo

[10] Ciberamenazas y Tendencias Edición 2017, CCN-CERT IA-16/17

Anexo 2 ENISA Threat Taxonomy[11]



[11] ENISA Threat Taxonomy, enero 2016

Anexo 3 Medidas de seguridad del ENS[12]

Marco organizativo	
org.1	Política de seguridad
org.2	Normativa de seguridad
org.3	Procedimientos de seguridad
org.4	Proceso de autorización

Marco operacional	
	Planificación
op.pl.1	Análisis de riesgos
op.pl.2	Arquitectura de seguridad
op.pl.3	Adquisición de nuevos componentes
op.pl.4	Dimensionamiento/Gestión de capacidades
op.pl.5	Componentes certificados
	Control de acceso
op.acc.1	Identificación
op.acc.2	Requisitos de acceso
op.acc.3	Segregación de funciones y tareas
op.acc.4	Proceso de gestión de derechos de acceso
op.acc.5	Mecanismo de autenticación
op.acc.6	Acceso local *(local logon)*
op.acc.7	Acceso remoto *(remote login)*
	Explotación
op.exp.1	Inventario de activos
op.exp.2	Configuración de seguridad
op.exp.3	Gestión de la configuración
op.exp.4	Mantenimiento
op.exp.5	Gestión de cambios
op.exp.6	Protección frente a código dañino
op.exp.7	Gestión de incidentes
op.exp.8	Registro de la actividad de los usuarios
op.exp.9	Registro de la gestión de incidentes
op.exp.10	Protección de los registros de actividad
op.exp.11	Protección de claves criptográficas
	Servicios externos
op.ext.1	Contratación y acuerdos de nivel de servicio
op.ext.2	Gestión diaria
op.ext.9	Medios alternativos
	Continuidad del servicio
op.cont.1	Análisis de impacto
op.cont.2	Plan de continuidad
op.cont.3	Pruebas periódicas
	Monitorización del sistema
op.mon.1	Detección de intrusión
op.mon.2	Sistema de métricas

Medidas de protección	
	Protección de las instalaciones e infraestructuras
mp.if.1	Áreas separadas y con control de acceso
mp.if.2	Identificación de las personas
mp.if.3	Acondicionamiento de los locales
mp.if.4	Energía eléctrica
mp.if.5	Protección frente a incendios
mp.if.6	Protección frente a inundaciones
mp.if.7	Registro de entrada y salida de equipamiento
mp.if.9	Instalaciones alternativas
	Gestión del personal
mp.per.1	Caracterización del puesto de trabajo
mp.per.2	Deberes y obligaciones
mp.per.3	Concienciación
mp.per.4	Formación
mp.per.9	Personal alternativo
	Protección de los equipos
mp.eq.1	Puesto de trabajo despejado
mp.eq.2	Bloqueo de puesto de trabajo
mp.eq.3	Protección de equipos portátiles
mp.eq.9	Medios alternativos
	Protección de las comunicaciones
mp.com.1	Perímetro seguro
mp.com.2	Protección de la confidencialidad
mp.com.3	Protección de la autenticidad y de la integridad
mp.com.4	Segregación de redes
mp.com.9	Medios alternativos
	Protección de los soportes de información
mp.si.1	Etiquetado
mp.si.2	Criptografía
mp.si.3	Custodia
mp.si.4	Transporte
mp.si.5	Borrado y destrucción
	Protección de las aplicaciones informáticas
mp.sw.1	Desarrollo
mp.sw.2	Aceptación y puesta en servicio
	Protección de la información
mp.info.1	Datos de carácter personal
mp.info.2	Calificación de la información
mp.info.3	Cifrado
mp.info.4	Firma electrónica
mp.info.5	Sellos de tiempo
mp.info.6	Limpieza de documentos
mp.info.9	Copias de seguridad (backup)
	Protección de los servicios
mp.s.1	Protección del correo electrónico
mp.s.2	Protección de servicios y aplicaciones web
mp.s.8	Protección frente a la denegación de servicio
mp.s.9	Medios alternativos

[12] Anexo II del ENS.

Anexo 4 Controles de Seguridad Críticos del CIS

Los controles de seguridad críticos (CSC) son un conjunto conciso y priorizado de acciones de ciberdefensa, orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible.

Incluyen un conjunto de 20 controles de seguridad de la información alineados con la publicación NIST[13] 800-53. En agosto de 2016 se publicó la versión 6.1, coordinada desde el Center for Internet Security (CIS).

Los controles están pensados para organizaciones de cualquier tipo, no obstante, el conocimiento de la organización y la exposición a las amenazas va a condicionar la propia priorización y alcance de la implantación de los controles. Según el CIS, con carácter general, las organizaciones que apliquen solo los cinco primeros CSC pueden reducir su riesgo de ciberataques alrededor del 85%. Si se implementan los 20 CSC el riesgo se puede reducir un 94%.

Estos controles pueden usarse como criterios de auditoría de referencia en las auditorías de ciberseguridad[14].

La siguiente tabla muestra los 20 Controles de Seguridad Críticos[15], así como los objetivos de control necesarios para su correcta implementación:

	Control	Objetivos de control	Comentarios
CSC 1	Inventario de dispositivos autorizados y no autorizados	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.	La revisión puede realizarse de dos formas: - Verificar que existe una gestión de inventarios hardware y software, identificando listas blancas y negras y su actualización (al ser una aproximación de "ver que existe un control", podríamos llamarla, "de capa 2"). - El auditor interno escanea las redes internas utilizando herramientas automáticas (actúa como Red Team, según el control 20, es decir, comportandose como lo haría un atacante), hace una "verificación técnica", que podríamos llamar "de capa 1". En el resto de controles también usaremos estas dos aproximaciones de revisión.
CSC 2	Inventario de software autorizado y no autorizado	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.	
CSC 3	Configuraciones seguras de software y hardware para dispositivos móviles, portátiles, equipos de sobremesa y servidores	Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables. *Ejemplos de buenas prácticas incluirán:* • *Implantar políticas robustas de autenticación para prevenir accesos no autorizados.* • *Eliminar software innecesario para limitar la exposición a vulnerabilidades.* • *Aplicar las actualizaciones de software y parches de seguridad para corregir vulnerabilidades conocidas.* • *Instalar antivirus en los servidores.*	Su revisión se puede enfocar, de forma complementaria a los controles 1 y 2, verificando si existe una política de bastionado de todos los dispositivos, aplicaciones y servicios, si esta política está alineada con buenas prácticas y si se dispone de un proceso de revisión de las vulnerabilidades que retroalimente la política de bastionado. Otra aproximación es que el auditor escanee los dispositivos/aplicaciones utilizando herramientas automatizadas, actuando como Red Team.
CSC 4	Proceso continuo de identificación y remediación de vulnerabilidades	Disponer un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	

[13] U.S. National Institute of Standards and Technology.

[14] Véase como ejemplo el informe del Auditor General of British Columbia de Octubre 2017, An Independent Audit of the Regional Transportation Management Centre's Cybersecurity Controls, basado en la revisión de los cinco primeros CSC.

[15] Fuente en español: Ciberseguridad. Una guía de supervisión (Instituto de Auditores Internos de España)

	Control	Objetivos de control	Comentarios
CSC 5	Control sobre privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	Este control nos lleva a que las cuentas de usuarios administradores de aplicaciones, dispositivos y sistemas operativos deben estar identificadas, su uso auditado, eliminando las que no se utilizan y cambiando las que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas. La revisión de este control puede orientarse a verificar la existencia de una política de alta, baja y mantenimiento de usuarios administradores, y la fortaleza de la contraseña (debería formar parte de la política de bastionado), y las tareas que se desarrollan para comprobar su cumplimiento. Por otro lado, también podemos solicitar el listado de usuarios definidos en los sistemas y los ficheros de contraseñas cifradas asociados, y comprobar que no disponen de las claves por defecto utilizando herramientas automáticas.
CSC 6	Mantenimiento y monitorización de los LOG de auditoría	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	Implica que todos los sistemas y aplicaciones deberían tener habilitadas las trazas de auditoría, incluyendo respuestas a desde dónde, quién, qué y cuándo, así como tener definidas acciones de alerta. Debería existir una política asociada, un formato de log corporativo y una tarea de análisis de logs. En organizaciones con presupuesto y personal suficiente se suele disponer de un SIEM (Security Information and Event Management), sistema que permite disponer en tiempo real de alertas de seguridad. La verificación pasa por analizar el contenido de los logs, y, si actuamos como Red Team, las actividades que realicemos, como escanear una red o conectarnos como usuario administrador desde un puesto no habitual, deberían reflejarse en los logs y generarse las alertas correspondientes.
CSC 7	Protección del correo electrónico y del navegador	Minimizar la posibilidad de que los atacantes manipulen a los empleados a través de su interacción con el correo electrónico y el navegador.	Pasa por utilizar clientes de correo y navegadores actualizados y evitar que el usuario pueda añadir extensiones, así como cambiar su configuración. La configuración debe ser la más restrictiva posible para que el usuario pueda trabajar, deshabilitando los plugins innecesarios. De forma complementaria, el control 8 habilita el análisis de malware en los equipos, y deben definirse medidas para evitar que el malware entre a través de la navegación del usuario o de la lectura de correo (IPS, antivirus de navegación y correo, bloqueo de URLs maliciosas, etc.).
CSC 8	Defensa contra el *malware*	Evitar la instalación, difusión y ejecución de código malicioso en distintos puntos al tiempo que se fomenta la automatización para permitir una actualización rápida en la defensa, recopilación de datos y la corrección.	Recomienda agregar otras medidas contra el malware que deben estar recogidas en la política, como el bloqueo de USB y la monitorización continúa de los equipos. Debe existir una política del uso seguro y de configuraciones autorizadas, y tareas de revisión automatizada de los equipos y servidores. Otra posible verificación pasa por enviar un correo con contenido no autorizado a una cuenta interna, o navegar por una página dentro de una lista negra.

	Control	Objetivos de control	Comentarios
CSC 9	Limitar y controlar los puertos de red, protoclos y servicios	Gestionar el uso de puertos, protocolos y servicios en los dispositivos que tengan red para reducir las vulnerabilidades disponibles a los atacantes.	Nos habla de limitar los servicios expuestos a las redes, y separar físicamente las máquinas que tienen esos servicios. Debe existir una política que defina que sólo los servicios y puertos necesarios para la organización estén habilitados, o restringidos a las redes/usuarios que realizan tareas asociadas. El resto debería estar deshabilitado/filtrado. La aproximación para verificar este control pasa por realizar escaneos automáticos de las diferentes redes, para identificar puertos/servicios que deberían estar restringidos o deshabilitados. Un auditor puede realizar esta tarea de forma puntual o verificar si existe un proceso continuo que lo realice.
CSC 10	Capacidad de recuperación de datos	Disponer procesos, metodologías y herramientas adecuadas para respaldar la información crítica y realizar pruebas de recuperación.	Nos pide que se hagan copias de seguridad de todos los datos críticos, así como que se verifique de forma periódica que estos se pueden recuperar en un tiempo asumible. Asimismo, los sistemas donde se guardan estas copias deben tener acceso restringido, tanto física como lógicamente. Para probar este control, se pueden solicitar las políticas de back up y el resultado de las pruebas de recuperación.
CSC 11	Configuraciones seguras de dispositivos de red (*firewalls*, *routers* y *switches*)	Establecer una configuración base para los dispositivos de infraestructura de red, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables.	Se basa en definir una configuración segura para los dispositivos de comunicaciones (firewalls, routers, switches), junto con los procesos de gestión de cambio asociados. Este control es la implantación para estos dispositivos de los controles 3, 4 y 5: configuración base segura, revisión de vulnerabilidades y control del uso del administrador y, adicionalmente, control de cuentas por defecto (control 16). El test de este control sería de la misma forma que los controles mencionados.
CSC 12	Defensa perimetral	Desarrollar una estrategia para detectar, prevenir y corregir los flujos de transmisión de información entre redes de distintos niveles de seguridad (confianza).	En este control vemos que tenemos que tener una seguridad perimetral basada en aplicar filtros sobre las comunicaciones de nuestra organización hacia y desde fuera, así como desplegar sensores que detecten actividades sospechosas y alimenten a nuestro SIEM, tenemos que protegernos, pero también es importante detectar si están intentando entrar o, si ya lo han hecho, identificarlos. Por otro lado, tenemos que tener una DMZ, una zona donde los servicios expuestos a Internet estén separados de la red interna. Si necesitamos acceder a la red interna desde fuera (teletrabajo), debemos implantar un segundo factor de autenticación. El análisis de las reglas de FW nos permite evaluar este control. De igual forma que en controles anteriores, podemos hacer un escaneo de nuestro perímetro desde Internet para identificar puntos de entrada, servicios accesibles sin autenticación robusta y, testear qué alertas han generado nuestra actividad.

	Control	Objetivos de control	Comentarios
CSC 13	Protección de los datos	Disponer de procesos y herramientas adecuadas para prevenir la fuga de información, mitigar los efectos cuando se ha producido un incidente de fuga de información, y asegurar la confidencialidad e integridad de la información sensible.	Este control confía en el cifrado de la información en reposo y en tránsito para garantizar la privacidad y prevenir una fuga.
CSC 14	Acceso basado en la necesidad de conocer (*need to know*)	El acceso a los activos críticos debe realizarse de acuerdo a una definición formal de qué personas, sistemas y aplicaciones tienen la necesidad y el derecho de acceso. Los procesos y herramientas utilizadas en el seguimiento, protección y corrección de estos accesos deben estar alineados con las definiciones.	El acceso a la información debe seguir el principio de "necesidad de conocer". Un perfilado adecuado mitiga el riesgo, pero aun así debemos implantar otros controles, ya que un ataque puede obtener credenciales que tienen acceso a la información. Debemos emprender acciones complementarias, y algunos de los controles que hemos visto nos ayudan: limitar el uso de USB, monitorizar las conexiones o la separación entre redes. La prueba del control tiene que ser empírica, intentar acceder a información a la que no tenemos acceso por perfil.
CSC 15	Control de acceso *wireless*	Disponer de procesos y herramientas para garantizar una seguridad adecuada en las redes WiFi y en los sistemas clientes, incluyendo seguimiento y corrección de las medidas de seguridad.	Nos dice que protejamos las redes wireless. Un inventario de todas las existentes, junto con revisiones periódicas por parte del área de seguridad de que no existen redes no autorizadas; la comprobación automática de sus vulnerabilidades y de la forta-leza de las contraseñas; y una limitación de las redes internas a las que se puede acceder; completan la revisión del control. Adicionalmente, se deberían desplegar detectores de intrusos en estas redes para identificar dispositivos no autorizados.
CSC 16	Control y monitorización de cuentas de sistema	Gestionar activamente el ciclo de vida de las cuentas de sistema y de aplicación (creación, uso, inactividad y borrado) para reducir su utilización por parte de un atacante.	Si el control 4 era qué hace el administrador, el 16 es si hay cuentas definidas en los sistemas que sean usuarios por defecto, usuarios que ya han abandonado la organización o si existen otras cuentas definidas en los sistemas. Por otro lado, se deben establecer bloqueos de cuentas por accesos fallidos (este punto debería estar en la política de seguridad), limitando desde dónde se puede acceder y solicitando un doble factor para acceder a sistemas/datos especialmente sensibles. Los accesos de terceros deben revisarse especialmente. Para probar este control, una opción es verificar que exista un proceso de revisión de usuarios. Otra opción es lanzar herramientas automáticas para identificar cuentas obsoletas habilitadas.

	Control	Objetivos de control	Comentarios
CSC 17	Verificación de las habilidades de seguridad y formación adecuada	Identificar los conocimientos específicos, habilidades y capacidades necesarias en la organización para la defensa de los activos críticos de la entidad, y desarrollar y evaluar un plan para identificar gaps y remediar con políticas, formación y programadas de sensibilización.	Se basa en que cada puesto funcional tiene que tener una formación específica en seguridad. Deben identificarse posibles carencias y formar a los empleados. Igualmente, la organización debería tener un programa de concienciación dirigido a todos los empleados, adecuado a las funciones que realizan. Solicitar la formación recibida del personal de seguridad nos permite identificar las carencias. Una forma de probar la efectividad es, una vez realizada la acción formativa/concienciadora, enviar un correo tipo phishing para ver la reacción del empleado y los pasos que realiza para denunciar el evento.
CSC 18	Seguridad en el ciclo de vida de las aplicaciones	Gestionar el ciclo de vida de todas las aplicaciones, tanto las desarrolladas internamente como las de proveedores para prevenir, detectar y corregir vulnerabilidades técnicas.	El ciclo de vida del software también necesita tener una capa de seguridad. Tanto el desarrollo interno como la compra de software de terceros requieren de una capa de seguridad. Las redes de desarrollo y producción deberían estar separadas. Unas directrices de programación segura o plan de formación específica de desarrollo seguro, ayuda a evitar vulnerabilidades en las aplicaciones desarrolladas internamente. Si lo acompañamos de una revisión automática de código por parte de herramientas especializadas, limitamos las vulnerabilidades. Una revisión final una vez integrado todo el desarrollo nos permite completar el ciclo. Existen productos que filtran/limitan las vulnerabilidades más comunes, que también pueden desplegarse en producción. Los productos de terceros deberían probarse antes de su implantación.
CSC 19	Gestión y respuesta a incidentes	Proteger la información y la reputación de la organización desarrollando e implementando una infraestructura de respuesta a incidentes para detectar un ataque, contener el daño de forma efectiva, expulsar al atacante, y restaurar la integridad de los sistemas y la red.	Se enfoca en la gestión de crisis. Es fundamental disponer de un plan de gestión y respuesta a incidentes que contemple procedimientos escritos, asignación de tareas y responsabilidades. Estos planes deberían ser probados para verificar cómo está preparada la organización frente a un incidente de envergadura, y garantizar una gestión adecuada a la crisis.
CSC 20	Realizar test de penetración y ejercicios de ataque	Probar las defensas de la organización (tecnología, procesos y personas) mediante la simulación de un ataque, utilizando sus mismas acciones y objetivos.	Nos habla de realizar ciberejercicios. Los tipos de ataques no paran de crecer. Aparecen nuevas técnicas de las que nos tenemos que defender. Una forma de probar si tenemos las defensas adecuadas es comportarnos como un posible atacante utilizando técnicas similares. La capa 2 puede realizar esta tarea. Auditoría Interna revisaría las situaciones identificadas y las acciones correctoras. Auditoría Interna también puede realizar la tarea (prueba todos los controles), o contratar los servicios de un externo.