
Guía práctica de fiscalización dos OCEX

GPF-OCEX 5311 Ciberseguridade, seguridade da información e auditoría externa

Referencia: GPF-OCEX 1315, 1500 e 5300

Documento elaborado pola Comisión Técnica dos OCEX e aprobado pola Conferencia de Presidentes de ASOCEX o 27/11/2017

1. Introducción	Páx 1
2. A ciberseguridade e a seguridade da información	Páx 2
3. Propiedades ou características da información dixital e da evidencia electrónica	Páx 3
4. Normas sobre seguridade da información e ciberseguridade	Páx 4
5. Consecuencias dun incidente de ciberseguridade	Páx 6
6. Ciber-resiliencia	Páx 7
7. Consideracións sobre ciberseguridade nas fiscalizacións dos OCEX	Páx 7
7.1 Auditorías operativas ou específicas de ciberseguridade ou de sistemas de información	Páx 7
7.2 Auditorías de seguridade da información en apoio de auditorías financeiras ou de cumprimento	Páx 8
8. Ciberseguridade e os CGTI	Páx 9
9. Selección dos controis relevantes para revisar nunha auditoría financeira	Páx 9
10. Os equipos de auditoría e a ciberseguridade	Páx 10
Anexo1 Ameazas máis significativas, tipoloxía das súas accións e as súas vítimas	Páx 11
Anexo 2 ENISA Threat Taxonomy	Pág 12
Anexo 3 Medidas de seguridade do ENS	Páx 13
Anexo 4 Controis de Seguridade Críticos do CIS	Páx 14

1. Introducción

Nos últimos anos acentuouse o fenómeno da xeneralización e crecente dependencia das tecnoloxías da información e as comunicacións (TIC) no desenvolvemento das actividades das administracións públicas, tanto nas súas relacións con cidadáns e provedores, como na súa xestión interna. Este feito orixinou que asistíssemos a un crecemento sen precedentes de ataques de moi distinto tipo, procedencia e obxectivos aos sistemas de información públicos e aos datos neles procesados e almacenados.

Nun mundo interconectado no que as distintas redes das administracións públicas non son senón elementos integrantes dunha rede global, os ciberriscos multiplícanse.

Vendo a amplitude das ameazas (axentes das ameazas máis significativos durante 2016, a tipoloxía das súas accións e as súas vítimas) sinaladas no informe do Centro Criptolóxico Nacional (CCN) “Ciberamenazas e Tendencias 2017” que se mostran no Anexo 1, ou revisando a taxonomía de ameazas de ciberseguridade publicada por ENISA que se mostra no Anexo 2, chégase á conclusión de que a ciberseguridade é unha materia moi importante, que debe ser abordada por todas as entidades públicas de forma integrada coas súas políticas de seguridade da información no seu sistema de control interno.

Actualmente a ciberseguridade converteuse nun dos temas máis relevantes tanto para os gobernos, como para os xestores públicos, e por suposto para os auditores públicos, dada a potencial repercusión que as ameazas á seguridade dos sistemas de información representan non só sobre as contas que se auditan se non á mesma continuidade na prestación de servizos públicos. O auditor público tamén debe ter en consideración as diversas normas legais que establecen obrigas nesta materia e cuxo cumprimento ten unha importancia paralela á dos controis que se establecen nelas.

O obxectivo da presente guía é servir de introdución á problemática que a ciberseguridade expón na actividade dos auditores dos OCEX, concienciar sobre a súa importancia e sinalar algunhas liñas de desenvolvemento posterior das GPF-OCEX.

2. A ciberseguridade e a seguridade da información

A Directiva 2016/1148 de Ciberseguridade define a *seguridade das redes e sistemas de información* (é dicir a ciberseguridade) como *a capacidade das redes e sistemas de información de resistir, cun nivel determinado de fiabilidade, toda acción que comprometa a **dispoñibilidade, autenticidade, integridade** ou **confidencialidade** dos datos almacenados, transmitidos ou tratados, ou os servizos correspondentes ofrecidos por tales redes e sistemas de información ou accesibles a través deles.*

Esta definición é coincidente coa do Esquema Nacional de Seguridade e contempla as **características fundamentais da información** que a ciberseguridade debe garantir. Xunto coa trazabilidade forman as cinco dimensións¹ de seguridade:

- A **dispoñibilidade** trata da capacidade dun servizo, un sistema ou unha información, a ser accesible e utilizable polos usuarios ou procesos autorizados cando estes requíranos.
- A **confidencialidade** é a propiedade da información, pola que se garante que está accesible unicamente a persoal autorizado a acceder a dita información.
- A **integridade** é a propiedade da información, pola que se garante a exactitude dos datos transportados ou almacenados, asegurando que non se produciu a súa alteración, perda ou destrución, xa sexa de forma accidental ou intencionada, por erros de software ou hardware ou por condicións ambientais.
- A **autenticidade** é a propiedade ou característica consistente en que unha entidade é quen di ser ou ben que garante a fonte da que proceden os datos.
- A **trazabilidade** é a propiedade ou característica consistente en que as actuacións dunha entidade poden ser imputadas exclusivamente a dita entidade.

Os conceptos de seguridade da información e ciberseguridade utilízanse frecuentemente de forma indistinta, pero existen uns matices que os diferencian. A seguridade da información trata da protección da información dentro dunha entidade, independentemente do seu formato. A ciberseguridade ocúpase especificamente da protección dos activos de información procesada, almacenada e transportada por **redes e sistemas de información interconectados**.

Un exemplo axudará a entender a diferenza. Nunha entidade pequena, que dispoña dun servidor para xestionar a súa contabilidade, nóminas, compras, etc, cunha rede interna que non estea conectada a internet, consideraremos na auditoría a problemática da seguridade da información, os CGTI e os controis de aplicación. Pero non haberá problemática relacionada coa ciberseguridade.

¹ A publicación do Centro Criptolóxico Nacional e da Federación Española de Municipios e Provincias, "[Guía estratéxica en seguridade para entidades locais](#)" de outubro de 2017, tenta aclarar este concepto:

"...en realidade, ¿que significa cada unha destas dimensións? Vexamos algúns exemplos:

- A **dispoñibilidade** actúa sobre a non interrupción do servizo (p.ex. A Web corporativa, perfil de contratante ou algúns trámites electrónicos na sede deixan de funcionar e non están accesibles a través de internet.)
- A **autenticidade** protexe o aseguramento da identidade (p.ex. A identidade da persoa que asinou un documento, quen se conectou a través dunha rede WIFI, etc.)
- A **confidencialidade** prevé a filtración de información (p.ex. Xestionar o acceso a determinado tipo de información.)
- A **integridade** prevé manipulacións da información (p.ex. Dispor de documentos que foron asinados de forma electrónica, asegurar a data de publicación dun documento na sede electrónica, etc.)
- A **trazabilidade** permite coñecer posibles rastros en accesos (p.ex. sistema de rexistro de accesos por parte de usuario, análise de posibles fugas de datos, intrusión a sistemas de ataques externos, etc.)"

A literatura internacional sobre a materia, en xeral, fala de tres dimensións ou características fundamentais da seguridade: confidencialidade, integridade e dispoñibilidade. O *WGITA-IDI Handbook on IT Audit for SAI* tamén, e sinala que a integridade está formada pola autenticidade e o non repudio. En definitiva as cinco dimensións do ENS só son unha extensión das tres fundamentais.

Nunha entidade de gran tamaño, con servizos aos cidadáns por internet, cunha administración electrónica desenvolvida, con múltiples localizacións xeográficas interconectadas, con servizos web que conectan cos provedores, etc, a problemática da ciberseguridade será unha área de risco e de especial consideración na auditoría.

O gran crecemento das **redes e sistemas de información interconectados** é o que orixinou que dentro do dominio da seguridade da información produciuse un crecente auxe dos temas relacionados coa ciberseguridade. Actualmente as ameazas á seguridade dos activos de información proveñen dun variado e crecente número de fontes, moitas delas a través de internet.

En todo caso, as políticas e controis de ciberseguridade deben estar aliñados coas políticas de seguridade da información das organizacións públicas e, pola súa transcendencia e impacto, o auditor público debe incluír na súa metodoloxía ordinaria de traballo a revisión dos controis de seguridade da información, incluíndo a ciberseguridade.

En síntese podemos dicir que **a finalidade da ciberseguridade é protexer os activos² de información procesada, almacenada e transportada por redes e sistemas de información interconectados.**

3. Propiedades ou características da información dixital e da evidencia electrónica

Acaba de sinalarse que a información e os datos que circulan, almacenan ou se procesan nun sistema de información deben ter unha serie de características que os controis de seguridade deben garantir, tal como require a Directiva de Ciberseguridade a nivel europeo.

Tamén, de acordo co previsto no Esquema Nacional de Seguridade os datos, informacións e servizos utilizados en medios electrónicos polas Administracións Públicas, deberán contar con medidas de seguridade que garantan o seu acceso, integridade, dispoñibilidade, autenticidade, confidencialidade, trazabilidade e conservación.

No marco dunha fiscalización, ditas características son esenciais para que a información e os datos obtidos en formato dixital polos auditores dos sistemas de información do ente auditado poidan considerarse evidencia fiable. Con esta finalidade **os auditores externos deben revisar os controis internos deseñados e implantados nos sistemas de información para garantir que os datos utilizados como fonte de evidencia teñen esas características.**

De acordo coa GPF-OCEX 1500 (apartado 37), os criterios, propiedades ou características que permitirán valorar a fiabilidade da información e garantir a mesma como evidencia de fiscalización nas contornas informatizadas son os seguintes:

- Autenticación: Refírese á posibilidade de confirmar, de forma indubitada, a identidade da persoa ou entidade que creou, orixinou ou da que procede a información (*Autenticidade*).
- Autorización: Refírese ao feito de que a información electrónica foi creada, procesada, gravada, corrixida, enviada, arquivada, ingresada e destruída só por persoas autorizadas e responsables.
- Confidencialidade: A información unicamente será coñecida polas persoas ou entidades autorizadas (quen a orixinan e a quen vai dirixida).
- Integridade: É a garantía de que os datos ou información de orixe foron validados e estes non foron alterados ao ser creados, procesados, transmitidos e almacenados nos sistemas informáticos.
- Dispoñibilidade: A información estará dispoñible para as persoas ou entidades autorizadas, evitándose as perdas de datos.
- Trazabilidade: Indica as accións ou procesos que levan a cabo no sistema, así como quen e cando as realiza.
- Non repudio: Imposibilidade de que unha persoa ou entidade que orixinase, transmitido ou recibido

² Enténdese por activo calquera información ou sistema relacionado co tratamento da mesma que teña valor para a organización, poden ser procesos de negocio, datos, aplicacións, equipos informáticos, persoal, soportes de información, redes, equipamento auxiliar ou instalacións.

información poida negar participar nesa orixe ou intercambio de datos. (*Segundo INCIBE, o non repudio pode considerarse sinónimo de autenticidade*).

Esta esixencia da GPF-OCEX 1500 está apoiada polo previsto nos artigos 17 da Lei 39/2015, de Procedemento Administrativo Común das Administracións Públicas e 46 da Lei 40/2015, Réxime Xurídico do Sector Público que establecen que os documentos administrativos almacenaranse por medios electrónicos e deberán conservarse nun formato que permita garantir a súa autenticidade, integridade, conservación, dispoñibilidade e accesibilidade.

Vemos que as propiedades que o auditor debe esixir á evidencia dixital son basicamente coincidentes coas características da información que o Esquema Nacional de Seguridade (en diante, ENS) pretende garantir.

Por tanto unha entidade que acredite o cumprimento co ENS, fundamentalmente mediante as auditorías de seguridade previstas no seu artigo 34, proporcionará aos auditores dos OCEX unha seguridade máis elevada que a que proporcione unha entidade que non acredite a súa conformidade co ENS.

Nestes últimos casos **os auditores deberán realizar procedementos adicionais para obter un determinado nivel de seguridade respecto da evidencia dixital que soporte os informes de fiscalización** (calquera que sexa o tipo de fiscalización realizada, financeira de legalidade ou operativa).

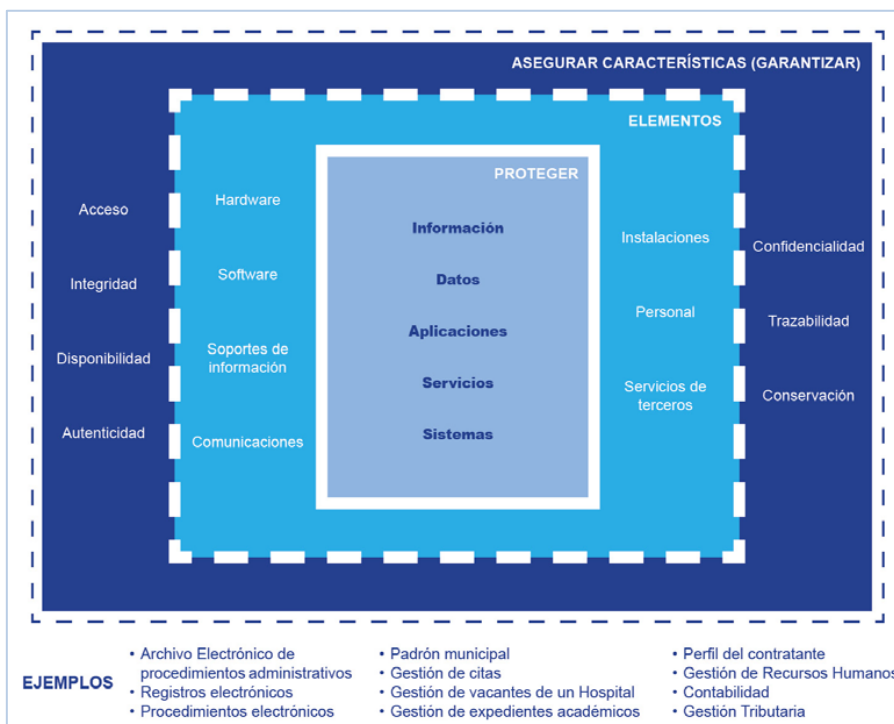
4. Normas sobre seguridade da información e ciberseguridade

En novembro de 2016 entraron en vigor no noso país as xa citadas leis 39/2015, e a 40/2015. Estas leis constitúen o eixo vertebrador das relacións dos cidadáns e as súas Administracións Públicas e destas entre si, consagrándose o uso das ferramentas electrónicas, baseadas en sistemas de información interconectados, como o medio habitual para canalizar tales relacións e o principio de **“dixital por defecto”** no funcionamento da Administración.

Segundo a Lei 40/2015, o Esquema Nacional de Seguridade ten por obxecto establecer a política de seguridade na utilización de medios electrónicos no ámbito de dita Lei, e está constituído polos principios básicos e requisitos mínimos que garantan adecuadamente a seguridade da información tratada.

O ENS, regulado no Real Decreto 3/2010, de 8 de xaneiro e actualizado polo Real Decreto 951/2015, de 23 de outubro, é o elemento normativo que pretende garantir a adecuada protección da información tratada e os servizos prestados polas entidades do sector público.

O ámbito de aplicación obxectivo ou material do ENS pode representarse no gráfico seguinte:



Fonte: Guía de seguridade (CCN-STIC-830) Ámbito de aplicación do ENS

A finalidade do ENS é a creación das condicións necesarias de confianza no uso dos medios electrónicos, a través de medidas para garantir a seguridade dos sistemas, os datos, as comunicacións, e os servizos electrónicos. Sinala que os sistemas de información prestarán os seus servizos e custodiarán a información de acordo coas súas especificacións funcionais, sen interrupcións ou modificacións fóra de control, e sen que a información poida chegar ao coñecemento de persoas non autorizadas.

No artigo 34 do ENS establécese que todas as entidades públicas están obrigadas a cumprir co ENS e someter os seus sistemas de información a unha auditoría regular ordinaria, polo menos cada dous anos, que verifique o cumprimento dos seus requirimentos. Tamén se deberá realizar unha auditoría con carácter extraordinario “sempre que se produzan modificacións substanciais no sistema de información, que poidan repercutir nas medidas de seguridade requiridas. A realización da auditoría extraordinaria determinará a data de cómputo para o cálculo dos dous anos, establecidos para a realización da seguinte auditoría regular ordinaria, indicados no parágrafo anterior.”

O obxectivo final desta auditoría de seguridade, realizada por expertos, é sustentar a confianza que merece o sistema auditado sobre o nivel de seguridade implantado, tanto internamente como fronte a terceiros, que puidesen estar relacionados; é dicir, calibrar a capacidade do sistema para garantir a integridade, dispoñibilidade, autenticidade, confidencialidade e trazabilidade dos servizos prestados e a información tratada, almacenada ou transmitida.

O artigo 41 do ENS sinala que: “Os órganos e Entidades de Dereito Público darán publicidade nas correspondentes sedes electrónicas ás declaracións de conformidade, e aos distintivos de seguridade dos que sexan acredores, obtidos respecto ao cumprimento do Esquema Nacional de Seguridade.”

Segundo a categoría do sistema distínguese entre:

- **Declaración de Conformidade:** de aplicación a sistemas de información de categoría **Básica**. Poderá representarse mediante Selo ou Distintivo de Declaración de Conformidade xerado pola entidade baixo cuxa responsabilidade estea o sistema.
- **Certificación de Conformidade:** de aplicación obrigatoria a sistemas de información de categoría **Media** ou **Alta** e voluntaria no caso de sistemas de información de categoría **Básica**. Os seus símbolos acreditativos son:



A progresiva implantación da Administración Electrónica fai que, ademais da estrita obriga legal de implantar o ENS, os OCEX deban considerar o risco, grande e crecente, que as cuestións relacionadas coa ciberseguridade teñen nos entes públicos, nas auditorías realizadas sobre eles, e na capacidade de reducir ditos riscos que ten unha adecuada implantación o ENS.

Por esta razón, o ENS adquire unha gran transcendencia e os OCEX deberán verificar nas fiscalizacións o cumprimento da legalidade en relación co ENS e se non se acredita a adecuación ao mesmo deberase reflectir no informe como **un incumprimento grave ou moi significativo**.

Por outra banda, o 6 de xullo de 2016 aprobouse a Directiva 2016/1148 do Parlamento Europeo e do Consello relativa ás medidas destinadas a garantir un elevado nivel común de seguridade das redes e sistemas de información na Unión, tamén coñecida como Directiva de Ciberseguridade ou Directiva NIS. Actualmente España está en proceso de transpoñer dita Directiva, que establece que os estados membros adoptarán e publicarán, como moi tarde o 9 de maio de 2018, as disposicións legais, regulamentarias e administrativas necesarias para dar cumprimento á mesma.

Outra norma con importante efecto sobre aspectos da confidencialidade da información, é o novo Regulamento Xeral de Protección de Datos da UE, aprobado o 27 de abril de 2016 e de plena aplicación para o sector público. Este RGPD será aplicable a partir do 25 de maio de 2018, data a partir da cal as políticas de seguridade da información e os controis internos deberán contemplar os seus requirimentos.

Nun nivel máis detallado, o Centro Criptolóxico Nacional, creado en 2004, que é a entidade que ten encomendada as funcións relativas á seguridade das tecnoloxías da información e de protección da información clasificada, elabora e difunde normas, instrucións, guías e recomendacións para garantir a seguridade dos sistemas TIC da Administración. Ditas guías son unha referencia esencial na materia.

5. Consecuencias dun incidente de ciberseguridade

Os incidentes de seguridade teñen un custo global, derivado de varios custos parciais: económicos directos, de servizo, de imaxe e reputación, por sancións, etc. Segundo o CCN os custos máis significativos dos ciberincidentes e a súa xestión son³:

- Tempo de inactividade

Perdas económicas e danos de reputación. No caso de empresas de servizos públicos, a falta de enerxía ou de auga podería afectar a millóns de persoas.

A principios de 2017, o troyano Wannacry provocou o peche temporal de sistemas enteiros de entes públicos e privados. Algunhas empresas de transporte público tiveron que paralizar a súa actividade. Tamén afectou gravemente ao sistema de saúde británico⁴.

Vulnerabilidades de ciberseguridade como a coñecida en xullo de 2017 sobre o servizo LEXNET provocou o peche temporal dese servizo esencial para a Administración de Xustiza. Ademais vulnerouse a confidencialidade de miles de datos persoais de especial protección.

- Custos económicos

Custos económicos: custos derivados da resposta a incidentes, responsabilidade económica fronte aos seus clientes e, mesmo, pago de sancións por motivos legais.

Relacionado co asunto LEXNET, o Consello de Ministros do 25 de agosto aprobou un investimento de 61 millóns de euros para melloras dos sistemas de información relacionados da Administración de Xustiza.

A Comisión Europea sinalou⁵ que a fraude cos pagos con tarxetas de crédito ascende polo menos a 1.400 millóns de euros na UE.

- Perda de datos

A perda de información persoal dos clientes ou propiedade intelectual, poden afectar as finanzas, a marca e a reputación. Os ciberdelincuentes poden ameazar con publicar datos roubados, nun intento de obter máis diñeiro da vítima.

Un dos sectores que máis está na diana dos ciberdelincuentes é o dos datos persoais relativos á saúde, área especialmente sensible e obxecto de protección especial.

- Perda de vidas

No caso dun hospital, a vida dos pacientes pode porse en risco⁶. Os rexistros, incluíndo historia clínica, poden quedar inaccesibles, o que provocaría atrasos no tratamento, a prescrición de medicamentos incorrectos, ou outros efectos potencialmente perniciosos.

A interrupción dos servizos prestados ao cidadán na actual contorna de administración electrónica representa non só custos para a administración senón para todos os cidadáns. Nestes casos poderíamos falar de Perdas de dereitos, en todos aqueles procedementos ou asuntos que teñan data límite de presentación (axudas sociais, presentación a oposicións, contratacións, etc).

As estimacións globais dos custos derivados das ciberamenazas realizados por diversos analistas ofrecen cifras elevadísimas.

³ [Ciberamenazas y Tendencias. Edición 2017, CCN-CERT IA-16/17. Resumen ejecutivo.](#)

⁴ Véxase o informe [Investigation: WannaCry cyber attack and the NHS](#), UK NAO, outubro de 2017.

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

⁶ Véxase o informe da UK NAO.

6. Ciber-resiliencia

A resiliencia é unha cualidade inherente a un organismo ou entidade, empresa ou estado que lle permite facer fronte a unha crise sen que a súa actividade véxase afectada. Así, a ciber-resiliencia é a habilidade para continuar proporcionando servizos ao mesmo tempo que se prevén, disuade e responde a ciberataques⁷. Tamén reduce a probabilidade de que estes ataques teñan éxito.

Ciber-resiliencia refírese xeralmente ás capacidades organizativas e técnicas para absorber impactos externos e internos, e recuperar a normalidade nas operacións dunha forma controlada.

A Estratexia de Ciberseguridade Nacional aprobada en 2013 inclúe a ciber-resiliencia nos seus dous primeiros obxectivos específicos, en particular o primeiro refírese ás administracións públicas da seguinte forma:⁸

“Obxectivo Garantir que os Sistemas de Información e Telecomunicacións que utilizan as Administracións Públicas posúen o adecuado nivel de ciberseguridade e resiliencia.”

Presumirase que unha entidade é ciber resiliente cando teña implementado un conxunto coherente e integrado de CGTI como o ENS.

7. Consideracións sobre ciberseguridade nas fiscalizacións dos OCEX

A ciberseguridade pode ser abordada nunha fiscalización de distintas formas, dependendo do obxectivo e alcance de cada fiscalización. Caben dous enfoques principais:

7.1 Auditorías operativas ou específicas de ciberseguridade ou de sistemas de información

Dependendo dos obxectivos e alcance da auditoría, poden exporse traballos como:

- Auditorías dos controis de ciberseguridade e de ciberresiliencia.
- Auditoría de seguridade da información.
- Auditoría de seguridade dos rexistros contables de facturas electrónicas.
- Auditoría dos sistemas de control interno automatizados.
- Auditoría dos controis de seguridade da receita electrónica.
- Etc.

Se se realiza unha auditoría informática non integrada nunha auditoría financeira, xeralmente todas as categorías de controis e todos os CGTI poden ser relevantes agás que expresamente exclúanse do alcance da auditoría.

Os obxectivos e alcances posibles son numerosos, e tan variados como se estableza na planificación xeral do OCEX. Un enfoque posible, podería consistir en revisar o cumprimento cos 20 Controis Críticos de Seguridade do Center for Internet Security (CIS) que se achegan no anexo 4.

Outro enfoque podería basearse en replicar total ou parcialmente as medidas de control previstas no ENS (ver Anexo 3).

⁷ “Ciber-resiliencia definiuse partindo da definición de resiliencia e restrinxindo as posibles fontes de crises a eventos tecnolóxicos e procedentes do ciberespazo, ou tamén se definiu limitando a dimensión afectada da empresa ao que son os seus sistemas de proceso de datos e as súas comunicacións. Dada a complexidade das organizacións, e a interdependencia entre os distintos elementos que as forman: persoal, contorna social, subministracións, infraestrutura TIC, procesos, ...; non se pode trazar unha liña divisoria clara entre o que supón a resiliencia da mesma e a ciber-resiliencia dos seus sistemas. Unha e outra están intimamente relacionadas, é máis, son un mesmo concepto. Non se pode crear unha infraestrutura tecnolóxica ciber-resiliente se a organización en si non é resiliente. A organización é un todo, e o departamento TIC non é un ente independente que pode sobrevivir ou pretender ser inmune aos eventos que poden sacudir ao seu persoal e os seus usuarios.” Luís de Salvador Carrasco, en [“Ciber-resiliencia”, Documento Opinión 35/2015](#), 3/4/2015, en [ieee.es](#).

⁸ [A UE tamén manifestou reiteradamente a súa preocupación pola ciberseguridade e a ciber-resiliencia.](#)

En xeral unha auditoría de ciberseguridade terá por finalidade determinar se se garanten as características fundamentais da información e o cumprimento da normativa. É dicir verificarase que:

- Están implantados os controis adecuados para garantir a integridade e a fiabilidade da información almacenada e procesada nos sistemas de información.
- A confidencialidade dos datos sensibles está protexida.
- A dispoñibilidade dos sistemas de información está asegurada.
- Existen controis que posibilitan unha adecuada trazabilidade das accións realizadas nos sistemas.
- O cumprimento das leis, regulamentos e estándares aplicables (de especial relevancia nas administracións públicas).

7.2 Auditorías de seguridade da información en apoio de auditorías financeiras ou de cumprimento

Os auditores responsables de cada auditoría deben analizar como afectan as cuestións relacionadas coa seguridade informática e a ciberseguridade aos obxectivos da súa auditoría. Canto maior sexa a entidade auditada e máis complexos os seus sistemas de información, maior impacto terán os aspectos tecnolóxicos e os riscos TIC, e maiores serán as consideracións ao respecto que deba facerse o auditor.

As GPF-OCEX 1315-1316/NIA-ES 315 requiren que nas auditorías financeiras de contas anuais ou de elementos das contas anuais (por exemplo: da conta xeral dun concello, da liquidación do orzamento, dos gastos de persoal, dos ingresos tributarios) o auditor obteña **un coñecemento suficiente sobre como utiliza o ente auditado os sistemas de información, sobre os controis automatizados e o seu impacto nos estados financeiros**. Isto inclúe revisar os CGTI (que basicamente están formados polos controis de seguridade da información e ciberseguridade) co alcance específico que se determine, en concordancia co alcance e obxectivos da auditoría.

Só tras adquirir ese coñecemento poderanse valorar os riscos de incorrección material nos estados financeiros, por exemplo, os riscos resultantes dun acceso non autorizado aos sistemas de información e dunha utilización e disposición non autorizados dos activos de información da entidade.

Nas auditorías dos sistemas de información en apoio dunha auditoría financeira, os expertos en seguridade TI analizarán cos auditores financeiros aqueles controis que son **relevantes para os obxectivos da auditoría financeira**, xa que non todos os riscos que pretenden mitigar os CGTI son iguais, nin en probabilidade, nin na súa materialidade. Para determinar que controis son relevantes deberase adoptar un enfoque baseado na análise do risco.

Os auditores deben coñecer os controis automatizados que teñen impacto no proceso de elaborar a información financeira incluíndo os controis xerais de tecnoloxía de información (CGTI), que están formados principalmente por controis relacionados coa seguridade da información e a ciberseguridade.

Por exemplo, se se audita o gasto da xestión da receita electrónica, unha parte importante do traballo debería ser abordado por auditores especializados que revisarán os sistemas de información relacionados coa receita electrónica, os CGTI e a ciberseguridade. O caso da xestión da receita electrónica é un exemplo moi claro da problemática da ciberseguridade xa que ese proceso está apoiado por un complexo conxunto de aplicacións e sistemas de información interrelacionados a través de redes públicas e privadas, con múltiples actores, no que os ciberriscos son moi elevados. Hoxe en día cibercriminosos poderían introducir recibos falsos no sistema sen necesidade de acudir a un médico ou unha farmacia e cobrar o diñeiro fraudulentamente obtido, comodamente sentados nunha cidade de Asia ou de América, suplantando as identidades electrónicas de facultativos e farmacias. Para evitar este tipo de fraude están os controis de ciberseguridade.

Seguindo con este exemplo, pódese afirmar que só o traballo conxunto e integrado de auditores financeiros e de sistemas dun OCEX, permite hoxe día fiscalizar este compoñente moi significativo do gasto sanitario. Como en moitos outros exemplos que se poderían pór, auditar doutra forma no século XXI non é posible.

O traballo dos expertos en seguridade da información, cando se realiza en apoio de auditorías financeiras ou de cumprimento, debe ser un traballo máis estruturado e estandarizado que o realizado en auditorías ad-hoc comentadas no apartado anterior, e debe de estar baseado na revisión dos CGTI seleccionados de acordo co enfoque de risco e das necesidades dos auditores financeiros, cos que se debe traballar de forma conxunta e integrada.

8. Ciberseguridade e os CGTI

A área que recolle o traballo de auditoría de sistemas de información que contempla os riscos e controis máis directamente relacionadas coa ciberseguridade é a relativa aos controis xerais das TI (CGTI).

De acordo coa metodoloxía en desenvolvemento pola Comisión Técnica dos OCEX, baseada nas NIA-ES, a revisión dos CGTI estrutúrase nas cinco categorías seguintes⁹:

- A. Marco organizativo
- B. Xestión de cambios en aplicacións e sistemas
- C. Operacións dos sistemas de información
- D. Controis de acceso a datos e programas
- E. Continuidade do servizo

A guía detallada de fiscalización dos CGTI, incluíndo os controis de seguridade e ciberseguridade, que está a elaborar a Comisión Técnica dos OCEX, estará aliñada na maior medida posible cos controis establecidos no ENS (véxase o Anexo 3), e por extensión co novo Regulamento Xeral de Protección de Datos (RGPD) da Unión Europea, que será de aplicación a partir do 25 de maio de 2018, de forma que se se acredita a efectiva adecuación ao ENS, coa auditoría de seguridade obrigatoria por exemplo, pódase reducir o alcance das probas de CGTI e ciberseguridade que deba realizar o OCEX, evitando desta forma molestias ao ente fiscalizado e realizando o noso traballo coa maior economía de recursos posible.

9. Selección dos controis relevantes para revisar nunha auditoría financeira

Debido ao gran número de CGTI que existen nunha entidade mediana ou grande **resulta materialmente imposible para un auditor revisalos na súa totalidade**. Ademais, gran parte deles non terán interese para os obxectivos da auditoría e só un pequeno subconxunto terá impacto sobre o risco de auditoría. É sobre este grupo de controis sobre os que debe centrarse a atención e o traballo do auditor.

Para seleccionar os controis internos a revisar, incluíndo os de ciberseguridade, o auditor de estados financeiros utilizará un enfoque de risco, de arriba-abaixo na auditoría do control interno, seguindo a metodoloxía da GPF-OCEX 1315. Para cada área ou aplicación significativa identificada requírese que:

- a) Valórense os riscos de incorrección material relacionados.
- b) Revísease a eficacia dos CGTI.

A importancia dos CGTI é tal, que do resultado da súa revisión dependerá a natureza, extensión e momento de realización das probas sobre os controis do proceso/aplicación e das probas substantivas.

- c) Revísease a eficacia dos controis do proceso/aplicación.
- d) Realícense as probas substantivas.

Este enfoque permitirá que o auditor se centre só nos controis que están relacionados cos sistemas e as aplicacións significativas a efectos da información contable, financeira ou orzamentaria auditada, de acordo cos obxectivos e alcance da auditoría que se estea realizando. É dicir, aqueles cuxo bo funcionamento afecta as aplicacións identificadas como significativas aos efectos da fiscalización. O resto carece de interese para a auditoría.

Se se revisan os CGTI dalgún sistema ou subsistema que non ten relación coa información contable, financeira ou orzamentaria auditada estarase a facer un traballo innecesario e por tanto ineficiente.

Por exemplo, se se está revisando unha aplicación de xestión de nóminas por ser os gastos de persoal unha área significativa, os procedementos de revisión dos controis xerais estarán focalizados naqueles que afectan máis directamente a esa aplicación. Neste caso non tería ningún interese revisar os controis relacionados co desenvolvemento e mantemento da aplicación de xestión do inventario de inmovilizado. Tampouco se revisarían os controis de acceso ou a xestión de usuarios da aplicación de ingresos, xa que eses traballos non

⁹ Esta estrutura, establecida no apartado 9.2 da CPF-OCEX 1316, é totalmente coherente co [Handbook on IT Audit](#) de INTOSAI.

nos permitirían reducir o risco de auditoría da área de gastos de persoal. Deberíanse revisar os CGTI relacionados coa aplicación de recursos humanos, coa de nóminas, as bases de datos de ambas aplicacións, e cos sistemas operativos e servidores que soportan ditas aplicacións e bases de datos.

Os ciberincidentes normalmente inicianse a través dos niveis/capas da rede perimetral e interna, que tenden a estar cada vez máis afastados/as das aplicacións, bases de datos e sistemas operativos que son os que, habitualmente, adóitanse incluír nas probas de controis de acceso aos sistemas que afectan os estados financeiros. A revisión de determinados controis, por exemplo a protección perimetral da rede fronte a intrusionas e os accesos á intranet, a revisión da configuración dos cortalumes existentes nos puntos de acceso ás redes corporativas, require perfís técnicos moi especializados nos equipos de auditoría de sistemas de información.

Tamén será importante revisar os controis de acceso lóxico (contrasinais, identificación e autenticación de usuarios), a xestión de usuarios das aplicacións significativas para a auditoría e das bases de datos subxacentes, e os cambios nos sistemas que poderían ter efectos nos estados financeiros. Unha típica proba de auditoría nesta área que consiste en verificar que os denominados “superusuarios” ou usuarios privilexiados están debidamente restrinxidos ao mínimo estritamente necesario e ademais que están debidamente controlados.

Se o número de aplicacións significativas é elevado, tal como sucede por exemplo na auditoría das contas dunha comunidade autónoma, será imposible revisar nunha fiscalización todos os controis de aplicación e CGTI relacionados con todas as aplicacións significativas. Nestes casos deseñase un plan de rotación da énfase, é dicir, un plan de auditoría plurianual que estableza un calendario para a revisión de forma rotativa dos controis automatizados, tanto de aplicación como xerais, que sexa factible realizar cos recursos do OCEX.

10. Os equipos de auditoría e a ciberseguridade

Para auditar entidades medianas ou grandes operando nunha contorna de administración electrónica deben formarse **equipos mixtos**, integrados por auditores financeiros e por especialistas en auditoría de sistemas de información e ciberseguridade, traballando conxuntamente con metodoloxía actualizada, de forma que se faga un traballo adaptado ás novas circunstancias moito máis eficaz e eficientemente.

Non facelo desta forma, non abordando os riscos relacionados coa seguridade da información e a ciberseguridade, supón aceptar uns riscos de auditoría ata niveis moi elevados.

Os OCEX deben estar preparados para afrontar a nova contorna e abordar os riscos relacionados coa ciberseguridade, xa que non só as actividades ordinarias realízanse a través de sistemas de información interconectados. As actividades fraudulentas, corruptas e delituosas, tamén se realizan cada vez máis por medios electrónicos aproveitando as vulnerabilidades que os sistemas de información das administracións públicas poidan ofrecer.

Ata que se incorporen ás plantillas dos OCEX auditores de sistemas de información e expertos en ciberseguridade, dispónse do recurso de contratar expertos externos para cubrir ese déficit de coñecementos e de profesionais especializados.

Por outra banda, posto que cada vez máis organizacións públicas confían no TIC para automatizar as súas operacións, a liña que separa o rol dos auditores de sistemas de información e o resto de auditores é cada vez máis difusa. O auditor financeiro é responsable de valorar os riscos de incorrección material nos estados financeiros, incluíndo os derivados de accesos non autorizados aos sistemas de información, polo que cada vez vaise a ter que relacionar máis extensamente co persoal de sistemas dos entes fiscalizados e terá que considerar persoalmente cuestións relacionadas coa seguridade da información.

En consecuencia, cada vez máis, o perfil do auditor financeiro vai requirir un maior compoñente tecnolóxico, aspecto este que deberá incorporarse nos mecanismos de acceso ás plantillas dos OCEX.

O persoal actual debe recibir continuas actividades formativas relacionadas coa administración electrónica, a seguridade da información, a ciberseguridade e o TIC en xeral.

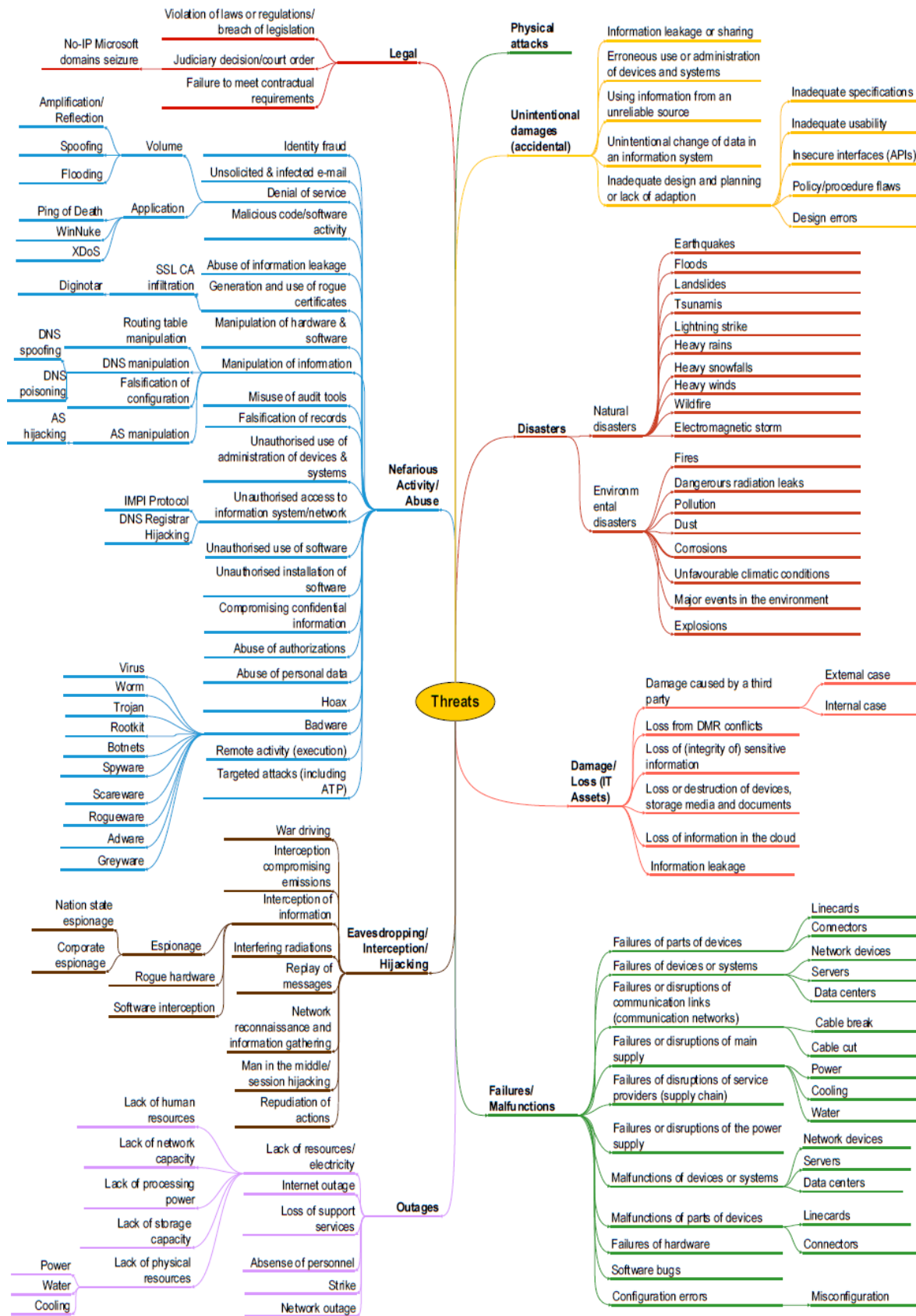
Anexo1 Ameazas máis significativas, tipoloxía das súas accións e as súas vítimas¹⁰

Axentes das ameazas	Vítimas		
	Sector Público	Organizacións privadas	Cidadáns
Estados	Ciberespionaxe político	Ciberespionaxe económico	Ciberespionaxe
	Capacidade ofensiva	Capacidade ofensiva	
Organizacións criminais	Roubo e publicación ou venda de información	Roubo e publicación ou venda de información	Roubo e publicación ou venda de información
	Manipulación da información	Manipulación da información	Manipulación da 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
Organizacións privadas		Ciberespionaxe industrial ou económico	Abuso ou revenda de información corporativa
Ciberterroristas	Disrupción / toma de control de sistemas	Disrupción / toma de control de sistemas	
Ciberyihadistas	Propaganda / Reclutamento	Propaganda / Reclutamento	Propaganda / Reclutamento
Ciberactivismo	Roubo e publicación de información	Roubo e publicación de información	
	Desfiguracións	Desfiguracións	
	Disrupción de sistemas	Disrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	
Ciber vándalos e script kiddies	Roubo de información	Roubo de información	Roubo de información
	Disrupción de sistemas	Disrupción de sistemas	
Actores internos	Roubo e publicación ou venda de información	Roubo e publicación ou venda de información	
	Disrupción de sistemas	Disrupción de sistemas	
Ciber-investigadores	Publicación de información	Publicación de información	

Código de cores:	<p>Non apareceron novas ameazas.</p> <p>ou</p> <p>Existen suficientes medidas para eliminar a ameaza</p> <p>ou</p> <p>Non existiron incidentes apreciábeis derivados da ameaza.</p>	<p>Observáronse novas tendencias ou fenómenos asociados coa ameaza.</p> <p>ou</p> <p>Existe un conxunto de medidas limitadas para eliminar a ameaza</p> <p>ou</p> <p>O número de incidentes derivados da ameaza non foi especialmente significativo</p>	<p>Existen claros desenvolvementos relacionados coa ameaza</p> <p>ou</p> <p>As medidas despregadas teñen un efecto limitado na ameaza</p> <p>ou</p> <p>O número de incidentes derivados da ameaza foi significativo</p>
------------------	---	---	---

¹⁰ Ciberameazas e Tendencias Edición 2017, CCN-CERT IA-16/17

Anexo 2 ENISA Threat Taxonomy¹¹



¹¹ ENISA Threat Taxonomy, xaneiro 2016

Anexo 3 Medidas de seguridade do ENS¹²

Marco organizativo	
org.1	Política de seguridade
org.2	Normativa de seguridade
org.3	Procedementos de seguridade
org.4	Proceso de autorización

Marco operacional	
Planificación	
op.pl.1	Análise de riscos
op.pl.2	Arquitectura de seguridade
op.pl.3	Adquisición de novos compoñentes
op.pl.4	Dimensionamento/Xestión de capacidades
op.pl.5	Compoñentes certificados
Control de acceso	
op.acc.1	Identificación
op.acc.2	Requisitos de acceso
op.acc.3	Segregación de funcións e tarefas
op.acc.4	Proceso de xestión de dereitos de acceso
op.acc.5	Mecanismo de autenticación
op.acc.6	Acceso local (<i>local login</i>)
op.acc.7	Acceso remoto (<i>remote login</i>)
Explotación	
op.exp.1	Inventario de activos
op.exp.2	Configuración de seguridade
op.exp.3	Xestión da configuración
op.exp.4	Mantemento
op.exp.5	Xestión de cambios
op.exp.6	Protección fronte a código daniño
op.exp.7	Xestión de incidentes
op.exp.8	Rexistro da actividade dos usuarios
op.exp.9	Rexistro da xestión de incidentes
op.exp.10	Protección dos rexistros de actividade
op.exp.11	Protección de claves criptográficas
Servizos externos	
op.ext.1	Contratación e acordos de nivel de servizo
op.ext.2	Xestión diaria
op.ext.9	Medios alternativos
Continuidade do servizo	
op.cont.1	Análise de impacto
op.cont.2	Plan de continuidade
op.cont.3	Probos periódicas
Monitorización do sistema	
op.mon.1	Detección de intrusión
op.mon.2	Sistema de métricas

Medidas de protección	
Protección das instalacións e infraestruturas	
mp.if.1	Áreas separadas e con control de acceso
mp.if.2	Identificación das persoas
mp.if.3	Acondicionamento dos locais
mp.if.4	Enerxía eléctrica
mp.if.5	Protección fronte a incendios
mp.if.6	Protección fronte a inundacións
mp.if.7	Rexistro de entrada e saída de equipamento
mp.if.9	Instalacións alternativas
Xestión do persoal	
mp.per.1	Caracterización do posto de traballo
mp.per.2	Deberes e obrigas
mp.per.3	Concienciación
mp.per.4	Formación
mp.per.9	Persoal alternativo
Protección dos equipos	
mp.eq.1	Posto de traballo despxado
mp.eq.2	Bloqueo de posto de traballo
mp.eq.3	Protección de equipos portátiles
mp.eq.9	Medios alternativos
Protección das comunicacións	
mp.com.1	Perímetro seguro
mp.com.2	Protección da confidencialidade
mp.com.3	Protección da autenticidade e da integridade
mp.com.4	Segregación de redes
mp.com.9	Medios alternativos
Protección dos soportes de información	
mp.se.1	Etiquetado
mp.se.2	Criptografía
mp.se.3	Custodia
mp.se.4	Transporte
mp.se.5	Borrado e destrución
Protección das aplicacións informáticas	
mp.sw.1	Desenvolvemento
mp.sw.2	Aceptación e posta en servizo
Protección da información	
mp.info.1	Datos de carácter persoal
mp.info.2	Cualificación da información
mp.info.3	Cifrado
mp.info.4	Firma electrónica
mp.info.5	Selos de tempo
mp.info.6	Limpeza de documentos
mp.info.9	Copias de seguridade (backup)
Protección dos servizos	
mp.s.1	Protección do correo electrónico
mp.s.2	Protección de servizos e aplicacións web
mp.s.8	Protección fronte á denegación de servizo
mp.s.9	Medios alternativos

¹² Anexo II do ENS.

Anexo 4 Controis de Seguridade Críticos do CIS

Os controis de seguridade críticos (CSC) son un conxunto conciso e priorizado de accións de ciberdefensa, orientados a mitigar os ataques máis comúns e danos coa intención de automatizalos o máximo posible.

Inclúen un conxunto de 20 controis de seguridade da información aliñados coa publicación NIST¹³ 800-53. En agosto de 2016 publicouse a versión 6.1, coordinada desde o Center for Internet Security (CIS).

Os controis están pensados para organizacións de calquera tipo, non obstante, o coñecemento da organización e a exposición ás ameazas vai condicionar a propia priorización e alcance da implantación dos controis. Segundo o CIS, con carácter xeral, as organizacións que apliquen só os cinco primeiros CSC poden reducir o seu risco de ciberataques ao redor do 85%. Se se implementan os 20 CSC o risco pódese reducir un 94%.

Estes controis poden usarse como criterios de auditoría de referencia nas auditorías de ciberseguridade¹⁴.

A seguinte táboa mostra os 20 Controis de Seguridade Críticos¹⁵, así como os obxectivos de control necesarios para a súa correcta implementación:

	Control	Obxectivos de control	Comentarios
CSC 1	Inventario de dispositivos autorizados e non autorizados	Xestionar activamente todos os dispositivos hardware na rede, de forma que só os dispositivos autorizados teñan acceso á rede.	A revisión pode realizarse de dúas formas: - Verificar que existe unha xestión de inventarios hardware e software, identificando listas brancas e negras e a súa actualización (ao ser unha aproximación de “ver que existe un control”, poderíamos chamala, “de capa 2”). - O auditor interno escanea as redes internas utilizando ferramentas automáticas (actúa como Rede Team, segundo o control 20, é dicir, comportándose como o faría un atacante), fai unha “verificación técnica”, que poderíamos chamar “de capa 1”.
CSC 2	Inventario de software autorizado e non autorizado	Xestionar activamente todo o software nos sistemas, de forma que só se poida instalar e executar software autorizado.	No resto de controis tamén usaremos estas dúas aproximacións de revisión.
CSC 3	Configuracións seguras de software e hardware para dispositivos móbiles, portátiles, equipos de sobremesa e servidores	Establecer unha configuración base segura para dispositivos móbiles, portátiles, equipos de sobremesa e servidores, e xestionalas activamente utilizando un proceso de xestión de cambios e configuracións rigoroso, para previr aos atacantes explotar servizos e configuracións vulnerables. <i>Exemplos de boas prácticas incluírán:</i> • <i>Implantar políticas robustas de autenticación para previr accesos non autorizados.</i> • <i>Eliminar software innecesario para limitar a exposición a vulnerabilidades.</i> • <i>Aplicar as actualizacións de software e parches de seguridade para corrixir vulnerabilidades coñecidas.</i> • <i>Instalar antivirus nos servidores.</i>	A súa revisión pódese enfocar, de forma complementaria aos controis 1 e 2, verificando se existe unha política de bastionado de todos os dispositivos, aplicacións e servizos, se esta política está aliñada con boas prácticas e se se dispón dun proceso de revisión das vulnerabilidades que retroalimente a política de bastionado. Outra aproximación é que o auditor escanee os dispositivos/aplicacións utilizando ferramentas automatizadas, actuando como Rede Team.
CSC 4	Proceso continuo de identificación e remediación de vulnerabilidades	Dispor un proceso continuo para obter información sobre novas vulnerabilidades, identificalas, remedialas e reducir a xanela de oportunidade aos atacantes.	

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

¹⁴ Véxase como exemplo o informe do Auditor Xeral of British Columbia de Outubro 2017, [An Independent Audit of the Rexional Transportation Management Centre’s Cybersecurity Controls](#), baseado na revisión dos cinco primeiros CSC.

¹⁵ Fonte en español: [Ciberseguridade. Unha guía de supervisión](#) (Instituto de Auditores Internos de España)

	Control	Obxectivos de control	Comentarios
CSC 5	Control sobre privilexios administrativos	Desenvolver procesos e utilizar ferramentas para identificar, previr e corrixir o uso e configuración de privilexios administrativos en computadores, redes e aplicacións.	<p>Este control lévanos a que as contas de usuarios administradores de aplicacións, dispositivos e sistemas operativos deben estar identificadas, o seu uso auditado, eliminando as que non se utilizan e cambiando as que están definidas por defecto. Adicionalmente, deben cumprir coa política de fortaleza de contrasinais.</p> <p>A revisión deste control pode orientarse a verificar a existencia dunha política de alta, baixa e mantemento de usuarios administradores, e a fortaleza do contrasinal (debería formar parte da política de bastionado), e as tarefas que se desenvolven para comprobar o seu cumprimento.</p> <p>Doutra banda, tamén podemos solicitar a listaxe de usuarios definidos nos sistemas e os ficheiros de contrasinais cifrados asociados, e comprobar que non dispoñen das claves por defecto utilizando ferramentas automáticas.</p>
CSC 6	Mantemento e monitorización dos LOG de auditoría	Recoller, xestionar e analizar logs de eventos que poden axudar a detectar, entender ou recuperarse dun ataque.	<p>Implica que todos os sistemas e aplicacións deberían ter habilitadas as trazas de auditoría, incluíndo respostas a desde onde, quen, que e cando, así como ter definidas accións de alerta.</p> <p>Debería existir unha política asociada, un formato de log corporativo e unha tarefa de análise de logs. En organizacións con orzamento e persoal suficiente adóitase dispor dun SIEM (Security Information and Event Management), sistema que permite dispor en tempo real de alertas de seguridade.</p> <p>A verificación pasa por analizar o contido dos logs, e, se actuamos como Rede Team, as actividades que realicemos, como escanear unha rede ou conectarnos como usuario administrador desde un posto non habitual, deberían reflectirse nos logs e xerarse as alertas correspondentes.</p>
CSC 7	Protección do correo electrónico e do navegador	Minimizar a posibilidade de que os atacantes manipulen aos empregados a través da súa interacción co correo electrónico e o navegador.	<p>Pasa por utilizar clientes de correo e navegadores actualizados e evitar que o usuario poida engadir extensións, así como cambiar a súa configuración. A configuración debe ser a máis restritiva posible para que o usuario poida traballar, deshabilitando os plugins innecesarios.</p> <p>De forma complementaria, o control 8 habilita a análise de malware nos equipos, e deben definirse medidas para evitar que o malware entre a través da navegación do usuario ou da lectura de correo (IPS, antivirus de navegación e correo, bloqueo de URLs maliciosas, etc.).</p>
CSC 8	Defensa contra o <i>malware</i>	Evitar a instalación, difusión e execución de código malicioso en distintos puntos á vez que se fomenta a automatización para permitir unha actualización rápida na defensa, recompilación de datos e a corrección.	<p>Recomenda agregar outras medidas contra o malware que deben estar recollidas na política, como o bloqueo de USB e a monitorización continua dos equipos.</p> <p>Debe existir unha política do uso seguro e de configuracións autorizadas, e tarefas de revisión automatizada dos equipos e servidores.</p> <p>Outra posible verificación pasa por enviar un correo con contido non autorizado a unha conta interna, ou navegar por unha páxina dentro dunha lista negra.</p>

	Control	Obxectivos de control	Comentarios
CSC 9	Limitar e controlar os portos de rede, protocolos e servizos	Xestionar o uso de portos, protocolos e servizos nos dispositivos que teñan rede para reducir as vulnerabilidades dispoñibles aos atacantes.	<p>Fálanos de limitar os servizos expostos ás redes, e separar fisicamente as máquinas que teñen eses servizos. Debe existir unha política que defina que só os servizos e portos necesarios para a organización estean habilitados, ou restrinxidos ás redes/usuarios que realizan tarefas asociadas. O resto debería estar deshabilitado/filtrado.</p> <p>A aproximación para verificar este control pasa por realizar escaneos automáticos das diferentes redes, para identificar portos/servizos que deberían estar restrinxidos ou deshabilitados. Un auditor pode realizar esta tarefa de forma puntual ou verificar se existe un proceso continuo que o realice.</p>
CSC 10	Capacidade de recuperación de datos	Dispor procesos, metodoloxías e ferramentas adecuadas para apoiar a información crítica e realizar probas de recuperación.	<p>Pídenos que se fagan copias de seguridade de todos os datos críticos, así como que se verifique de forma periódica que estes se poden recuperar nun tempo asumible. Así mesmo, os sistemas onde se gardan estas copias deben ter acceso restrinxido, tanto física como lóxicamente.</p> <p>Para probar este control, pódense solicitar as políticas de back up e o resultado das probas de recuperación.</p>
CSC 11	Configuracións seguras de dispositivos de rede (<i>firewalls, routers e switches</i>)	Establecer unha configuración base para os dispositivos de infraestrutura de rede, e xestionalas activamente utilizando un proceso de xestión de cambios e configuracións rigoroso, para previr aos atacantes explotar servizos e configuracións vulnerables.	<p>Baséase en definir unha configuración segura para os dispositivos de comunicacións (<i>firewalls, routers, switches</i>), xunto cos procesos de xestión de cambio asociados. Este control é a implantación para estes dispositivos dos controis 3, 4 e 5: configuración base segura, revisión de vulnerabilidades e control do uso do administrador e, adicionalmente, control de contas por defecto (control 16).</p> <p>O test deste control sería da mesma forma que os controis mencionados.</p>
CSC 12	Defensa perimetral	Desenvolver unha estratexia para detectar, previr e corrixir os fluxos de transmisión de información entre redes de distintos niveis de seguridade (confianza).	<p>Neste control vemos que temos que ter unha seguridade perimetral baseada en aplicar filtros sobre as comunicacións da nosa organización cara e desde fóra, así como despregar sensores que detecten actividades sospeitosas e alimenten ao noso SIEM, temos que protexernos, pero tamén é importante detectar se están a tentar entrar ou, se xa o fixeron, identificalos.</p> <p>Doutra banda, temos que ter unha DMZ, unha zona onde os servizos expostos a Internet estean separados da rede interna.</p> <p>Se necesitamos acceder á rede interna desde fóra (teletraballo), debemos implantar un segundo factor de autenticación.</p> <p>A análise das regras de FW permítenos avaliar este control. De igual forma que en controis anteriores, podemos facer un escaneo do noso perímetro desde Internet para identificar puntos de entrada, servizos accesibles sen autenticación robusta e, testear que alertas xeraron a nosa actividade.</p>
CSC 13	Protección dos datos	Dispor de procesos e ferramentas adecuadas para previr a fuga de información, mitigar os efectos cando se produciu un incidente de fuga de información, e asegurar a confidencialidade e integridade da información sensible.	<p>Este control confía no cifrado da información en repouso e en tránsito para garantir a privacidade e previr unha fuga.</p>

	Control	Obxectivos de control	Comentarios
CSC 14	Acceso baseado na necesidade de coñecer (<i>need to know</i>)	O acceso aos activos críticos debe realizarse de acordo a unha definición formal de que persoas, sistemas e aplicacións teñen a necesidade e o dereito de acceso. Os procesos e ferramentas utilizadas no seguimento, protección e corrección destes accesos deben estar aliñados coas definicións.	<p>O acceso á información debe seguir o principio de “necesidade de coñecer”. Un perfilado adecuado mitiga o risco, pero aínda así debemos implantar outros controis, xa que un ataque pode obter credenciais que teñen acceso á información. Debemos emprender accións complementarias, e algúns dos controis que vimos axudándonos: limitar o uso de USB, monitorizar as conexións ou a separación entre redes.</p> <p>A proba do control ten que ser empírica, tentar acceder a información á que non temos acceso por perfil.</p>
CSC 15	Control de acceso <i>wireless</i>	Dispor de procesos e ferramentas para garantir unha seguridade adecuada nas redes Wifi e nos sistemas clientes, incluíndo seguimento e corrección das medidas de seguridade.	<p>Dinos que protexamos as redes wireless. Un inventario de todas as existentes, xunto con revisións periódicas por parte da área de seguridade de que non existen redes non autorizadas; a comprobación automática das súas vulnerabilidades e da forza dos contraseñais; e unha limitación das redes internas ás que se pode acceder; completan a revisión do control.</p> <p>Adicionalmente, deberíanse despregar detectores de intrusos nestas redes para identificar dispositivos non autorizados.</p>
CSC 16	Control e monitorización de contas de sistema	Xestionar activamente o ciclo de vida das contas de sistema e de aplicación (creación, uso, inactividade e borrado) para reducir a súa utilización por parte dun atacante.	<p>Se o control 4 era que fai o administrador, o 16 é se hai contas definidas nos sistemas que sexan usuarios por defecto, usuarios que xa abandonaron a organización ou se existen outras contas definidas nos sistemas.</p> <p>Doutra banda, débense establecer bloqueos de contas por accesos fallidos (este punto debería estar na política de seguridade), limitando desde onde se pode acceder e solicitando un dobre factor para acceder a sistemas/datos especialmente sensibles.</p> <p>Os accesos de terceiros deben revisarse especialmente.</p> <p>Para probar este control, unha opción é verificar que exista un proceso de revisión de usuarios. Outra opción é lanzar ferramentas automáticas para identificar contas obsoletas habilitadas.</p>
CSC 17	Verificación das habilidades de seguridade e formación adecuada	Identificar os coñecementos específicos, habilidades e capacidades necesarias na organización para a defensa dos activos críticos da entidade, e desenvolver e avaliar un plan para identificar gaps e remediar con políticas, formación e programadas de sensibilización.	<p>Baséase en que cada posto funcional ten que ter unha formación específica en seguridade. Deben identificarse posibles carencias e formar aos empregados. Igualmente, a organización debería ter un programa de concienciación dirixido a todos os empregados, adecuado ás funcións que realizan.</p> <p>Solicitar a formación recibida do persoal de seguridade permítenos identificar as carencias.</p> <p>Unha forma de probar a efectividade é, unha vez realizada a acción formativa/concienciadora, enviar un correo tipo phishing para ver a reacción do empregado e os pasos que realiza para denunciar o evento.</p>

	Control	Obxectivos de control	Comentarios
CSC 18	Seguridade no ciclo de vida das aplicacións	Xestionar o ciclo de vida de todas as aplicacións, tanto as desenvolvidas internamente como as de provedores para previr, detectar e corrixir vulnerabilidades técnicas.	<p>O ciclo de vida do software tamén necesita ter unha capa de seguridade. Tanto o desenvolvemento interno como a compra de software de terceiros requiren dunha capa de seguridade.</p> <p>As redes de desenvolvemento e produción deberían estar separadas.</p> <p>Unhas directrices de programación segura ou plan de formación específica de desenvolvemento seguro, axuda a evitar vulnerabilidades nas aplicacións desenvolvidas internamente. Se o acompañamos dunha revisión automática de código por parte de ferramentas especializadas, limitamos as vulnerabilidades.</p> <p>Unha revisión final unha vez integrado todo o desenvolvemento permítenos completar o ciclo.</p> <p>Existen produtos que filtran/limitan as vulnerabilidades máis comúns, que tamén poden desprezarse en produción.</p> <p>Os produtos de terceiros deberían probarse antes da súa implantación.</p>
CSC 19	Xestión e resposta a incidentes	Protexer a información e a reputación da organización desenvolvendo e implementando unha infraestrutura de resposta a incidentes para detectar un ataque, conter o dano de forma efectiva, expulsar ao atacante, e restaurar a integridade dos sistemas e a rede.	<p>Enfócase na xestión de crise. É fundamental dispor dun plan de xestión e resposta a incidentes que contemple procedementos escritos, asignación de tarefas e responsabilidades.</p> <p>Estes plans deberían ser probados para verificar como está preparada a organización fronte a un incidente de envergadura, e garantir unha xestión adecuada á crise.</p>
CSC 20	Realizar test de penetración e exercicios de ataque	Probar as defensas da organización (tecnoloxía, procesos e persoas) mediante a simulación dun ataque, utilizando as súas mesmas accións e obxectivos.	<p>Fálanos de realizar ciberexercicios. Os tipos de ataques non pairan de crecer. Aparecen novas técnicas das que nos temos que defender. Unha forma de probar se temos as defensas adecuadas é comportarnos como un posible atacante utilizando técnicas similares.</p> <p>A capa 2 pode realizar esta tarefa. Auditoría Interna revisaría as situacións identificadas e as accións correctoras.</p> <p>Auditoría Interna tamén pode realizar a tarefa (proba todos os controis), ou contratar os servizos dun externo.</p>