GPF-OCEX 5330 Revisión dos controis xerais de tecnoloxías de información nunha contorna de administración electrónica

Referencia: ISSAI 5300, GPF-OCEX 5300, GPF-OCEX 1315 e GPF-OCEX 1316

Documento elaborado pola Comisión Técnica dos OCEX e aprobado pola Conferencia de Presidentes de ASOCEX o 12/11/2018

1. Introdución

O enfoque de auditoría baseado na análise do risco é o fundamento central da actividade auditora desenvolvida baixo as Normas Internacionais de Auditoría (NIA-ES) e as ISSAI-ES. Tal como sinala a GPF-OCEX 1315, "de acordo con este enfoque, o obxectivo do auditor é obter unha seguridade razoable de que as contas anuais no seu conxunto están libres de incorreccións materiais, debidas a fraude ou erro. Unha seguridade razoable é un grao alto de seguridade e alcánzase cando o auditor obtivo evidencia de auditoría suficiente e adecuada para reducir o risco de auditoría (é dicir, o risco de expresar unha opinión inadecuada cando as contas anuais conteñan incorreccións materiais) a un nivel aceptablemente baixo. Con todo, unha seguridade razoable non significa un grao absoluto de seguridade, debido a que existen limitacións inherentes á auditoría que fan que a maior parte da evidencia de auditoría a partir da cal o auditor alcanza as súas conclusións e na que basea a súa opinión sexa máis convincente que concluínte."

Actualmente, nunha auditoría financeira baseada na análise dos riscos realizada de acordo coa ISSAI-ES 200, o estudo e revisión dos sistemas de información nos que se sustenta a xestión dunha entidade (empresa ou fundación pública, concello, administración da comunidade autónoma, etc.) converteuse nunha actividade de importancia crecente, na medida en que esa xestión se apoia nuns sistemas de información interconectados que, coa plena implantación da administración electrónica, foron adquirindo unha complexidade cada vez maior. Esta situación xerou unha serie de novos e importantes riscos de auditoría (inherentes e de control) que deben ser considerados na estratexia de auditoría.

Para orientar e facilitar aos auditores dos OCEX a aplicación do enfoque de risco e a auditoría en contornas de administración electrónica desenvolvéronse as Guías Prácticas de Fiscalización (GPF-OCEX).

De acordo coas ISSAI-ES/NIA-ES, unha vez adquirido un coñecemento xeral da entidade, incluíndo os seus sistemas de información e de control interno, e antes de iniciar a revisión dos procesos e aplicacións de xestión significativos para os efectos da auditoría financeira e dos seus controis, débese revisar a situación dos controis xerais, xa que o grao de confianza nos mesmos determinará a posterior estratexia de auditoría.

Nunha contorna informatizada de complexidade media ou alta, a revisión dos controis xerais de tecnoloxías da información (CXTI) requirirá, normalmente, a colaboración dun experto en auditoría de sistemas de información e a aplicación dunha metodoloxía específica. Nestas circunstancias a revisión dos CXTI (e dos controis de aplicación) é un procedemento indispensable para reducir os riscos de auditoría a un nivel aceptable.

Moi esquemáticamente, as etapas dunha auditoría executada co enfoque baseado na análise dos riscos son (ver GPF-OCEX 1315) as que se mostran na figura 1.

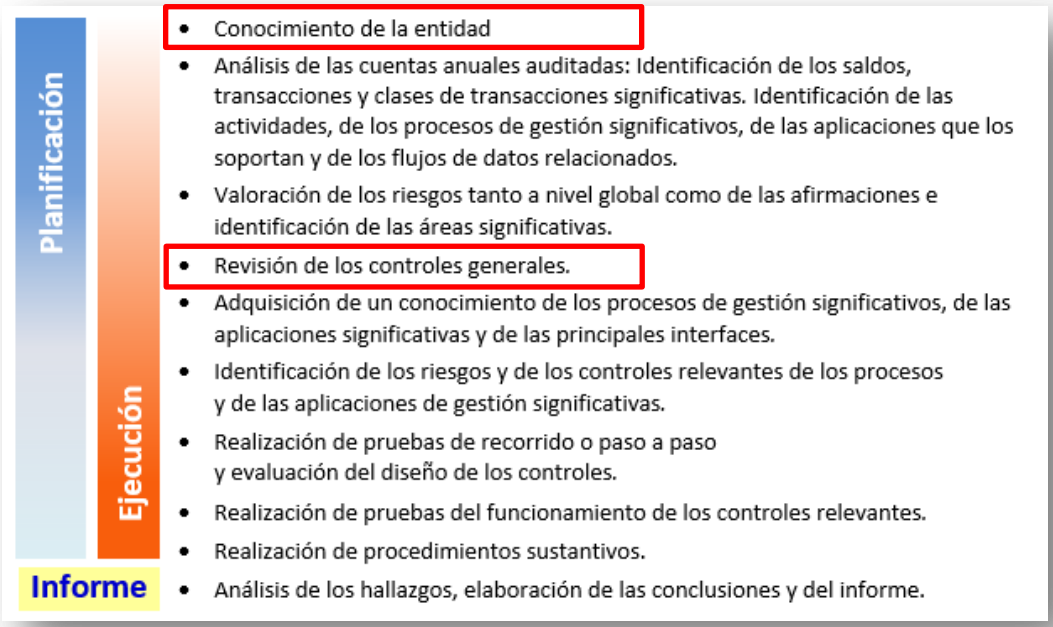

Figura 1

No Anexo 4 da GPF-OCEX 1315 pode verse un fluxograma da actividade típica nunha auditoría financeira.

As normas reguladoras da auditoría pública máis recentes recollen a necesidade de que os auditores revisen a fiabilidade dos sistemas de información, dos controis internos e da seguridade da información[1].

Para a adecuada comprensión desta guía debe lerse previamente a GPF-OCEX 1315 e a GPF-OCEX 1316.

Para revisar os CXTI será indispensable que o equipo de fiscalización conte coa colaboración de especialistas en auditoría de sistemas de información, ben persoal propio do OCEX ou ben expertos externos contratados.

No desenvolvemento desta GPF-OCEX 5330, cuxo contido está fundamentalmente relacionado coa auditoría da seguridade da información, tívose especial coidado en manter a máxima coherencia cos postulados do ENS

[1] A modo de exemplo:

a) A Lei 16/2017 que modifica a Lei 6/1985, do 11 de maio, de Sindicatura de Comptes da Comunitat Valenciana establece:

"Artigo 11. Medios de información para o exercicio da función fiscalizadora e consecuencias derivadas da obstrución ao exercicio da actividade fiscalizadora.

Un. No desenvolvemento da súa función fiscalizadora, a Sindicatura de Comptes está facultada para: …

*d) **Verificar a seguridade e fiabilidade dos sistemas informáticos** que soportan a información económico-financeira, contable e de xestión."*

b) O Real Decreto 424/2017, do 28 de abril, polo que se regula o réxime xurídico do control interno nas entidades do Sector Público Local establece:

"CAPÍTULO III Da auditoría pública

Artigo 33. Execución das actuacións de auditoría pública.

4. Para a aplicación dos procedementos de auditoría poderán desenvolverse as seguintes actuacións: …

*e) **Verificar a seguridade e fiabilidade dos sistemas informáticos** que soportan a información económico-financeira e contable."*

c) A Resolución do 30 de xullo de 2015, da Intervención Xeral da Administración do Estado, pola que se ditan instrucións para o exercicio da auditoría pública, establece:

"Duodécima. Procedementos para o exercicio da auditoría pública.

2. Para a aplicación dos procedementos de auditoría poderán desenvolverse as seguintes actuacións:

*e) **Verificar a seguridade e fiabilidade dos sistemas informáticos** que soportan a información económico-financeira e contable."*

debido a que é de obrigado cumprimento para todos os entes públicos e esta aliñación facilita a realización das auditorías de CXTI e coadxuvan á implantación do ENS.

2. Obxectivos desta etapa da auditoría

A revisión dos controis xerais TI como finalidade:

- Adquirir ou corroborar un coñecemento xeral da estrutura e organización dos sistemas de información da entidade e un coñecemento profundo daqueles que afectan os procesos de xestión significativos que van ser revisados.
- Identificar, analizar e comprobar o adecuado funcionamento dos controis xerais.
- Confirmar se a estratexia de auditoría adoptada na planificación é válida.
- Reducir o risco de auditoría a un nivel aceptable.

O **obxectivo da auditoría** dos CXTI será obter unha seguridade razoable de que o sistema de control interno proporciona unha seguridade razoable sobre a confidencialidade, integridade, autenticidade, dispoñibilidade, e trazabilidade dos datos, a información e os activos dos sistemas de información.

3. Concepto de control xeral

3.1 Os controis xerais son as políticas e procedementos que se aplican á totalidade ou a gran parte dos sistemas de información dunha entidade, incluíndo a infraestrutura e plataformas TI da organización auditada e axudan a asegurar o seu correcto funcionamento.

Os controis xerais de tecnoloxías da información (CXTI) son aqueles controis relacionados co uso das tecnoloxías da información e as comunicacións (TIC) implantados nos distintos niveis da estrutura organizativa xeral dunha institución e nos seus sistemas de información, que establecen un marco xeral de confianza respecto do funcionamento do resto de controis implantados nos procedementos e aplicacións informáticas de xestión.

A súa importancia radica en que teñen un efecto xeneralizado, é dicir, adoitan afectar a máis dunha aplicación informática, e se os CXTI non funcionan adecuadamente imposibilítase que se poida confiar nos controis dos procedementos e aplicacións de xestión.

3.2 A finalidade dos controis xerais dunha contorna informatizada é establecer un marco xeral de control e confianza sobre as actividades do sistema informático e asegurar razoablemente a consecución dos obxectivos xerais de control interno e o correcto funcionamento dos controis de aplicación.

3.3 Desde o punto de vista do auditor **os obxectivos dos CXTI son proporcionar unha garantía razoable de que os datos, a información e os activos dos sistemas de información cumpren as seguintes propiedades,** que coinciden coas cinco dimensións da seguridade da información que establece o Esquema Nacional de Seguridade**:**

- **Confidencialidade**, é a propiedade da información pola que se garante que está accesible unicamente a persoal autorizado a acceder a dita información.
- **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.
- **Dispoñibilidade**, trátase da capacidade dun servizo, un sistema ou unha información, de ser accesible e utilizable polos usuarios ou procesos autorizados cando estes o requiran.
- **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.
- **Trazabilidade**, é a propiedade ou característica consistente en que as actuacións dunha entidade poden ser imputadas exclusivamente a dita entidade.

3.4 A finalidade da auditoría dos CXTI é verificar a súa eficacia, é dicir que garanten razoablemente estas propiedades. Para poder confiar nos controis implantados nas aplicacións informáticas é requisito fundamental que os controis xerais da contorna de TI sexan efectivos e, por tanto, permitan garantir o bo funcionamento daqueles. En caso contrario, non se poderá confiar nos controis automáticos embebidos nas mesmas.

Tomando en consideración os diferentes niveis que conforman os sistemas de información, a revisión dos CXTI estrutúrase nas áreas que se detallan no apartado 5 seguinte.

3.5 Para os efectos desta guía, podemos representar o sistema de información dunha entidade mediante un modelo simplificado formado por cinco niveis ou capas tecnolóxicas superpostas, tal como se mostra na figura 2.

Debemos facer unha primeira distinción moi importante entre[2]:

- Os **controis xerais das tecnoloxías da información (CXTI).** Afectan a todos os niveis dos sistemas de información, aínda que están relacionados con moita maior intensidade con aqueles niveis de carácter xeral que afectan a toda a organización e aos sistemas TI. Son políticas e procedementos vinculados a moitas aplicacións e favorecen un funcionamento eficaz dos controis das aplicacións.
- Os **controis de aplicación.** Operan ao nivel dos procesos de xestión e que se aplican ao procesamento das transaccións mediante aplicacións informáticas específicas. Son analizados na GPF-OCEX 5340.

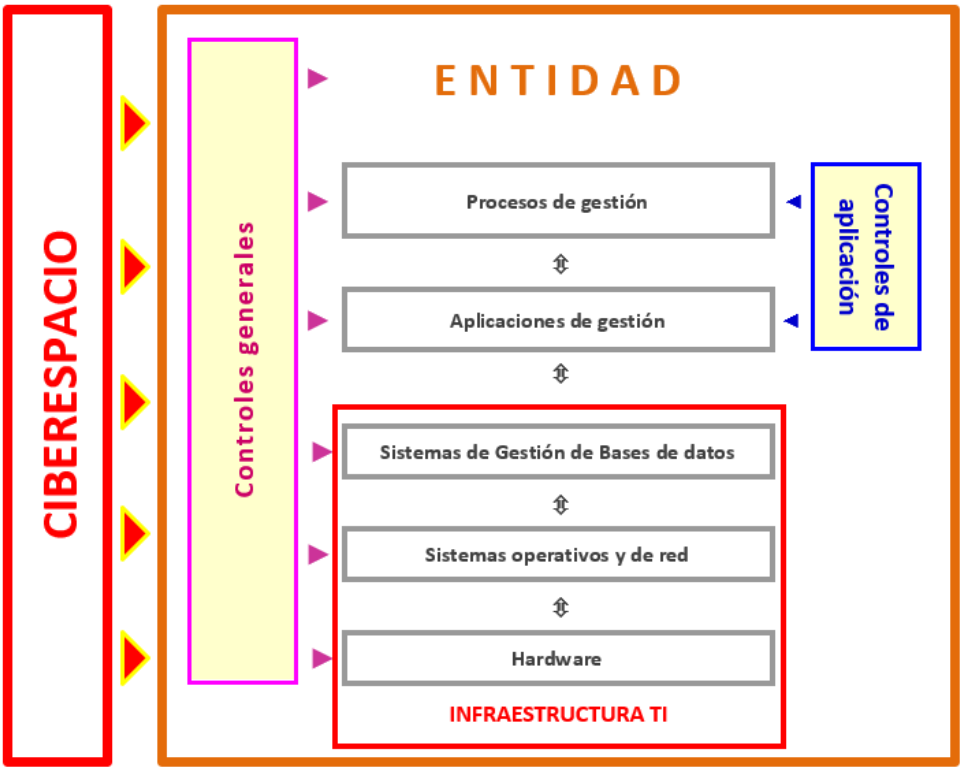

Figura 2

[2] Véxase GPF-OCEX 1316; apartado 9.2.

3.6 Os CXTI poden establecerse nos seguintes niveis:

a) Nivel da entidade

Os controis a este nivel reflíctense na forma de funcionar dunha organización, e inclúen políticas, procedementos e outras prácticas de alto nivel que marcan as pautas da organización incluíndo as materias relacionadas coas TIC. Forman a contorna ou ambiente de control dunha entidade e son un compoñente fundamental do modelo COSO[3].

O ambiente ou contorna de control e o compromiso con comportamentos éticos é unha "filosofía" de traballo que debe emanar de arriba cara abaixo, desde os altos postos directivos cara ao resto da organización. É esencial que o ton adecuado de control sexa marcado polos máximos responsables da entidade, que se envíe unha mensaxe a toda a organización de que os controis deben ser tomados en serio.

Os controis a nivel de entidade teñen influencia significativa sobre o rigor co que o sistema de control interno é deseñado e opera no conxunto dos procesos. A existencia duns CXTI rigorosos a este nivel, como son, por exemplo, unhas políticas e procedementos ben definidos e comunicados, con frecuencia suxiren unha contorna operativa TI máis fiable.

En sentido contrario, as organizacións cuns controis débiles a este nivel é máis probable que teñan dificultades á hora de realizar actividades de control regularmente. Por conseguinte, a fortaleza ou debilidade dos controis a nivel de entidade terá o seu efecto na natureza, extensión e momento en que se realicen as probas de auditoría.

A capacidade da dirección para eludir controis e un pobre ton de control (que se manifesta a nivel da entidade) son dous aspectos comúns nun mal comportamento corporativo.

Unha sólida comprensión dos controis a este nivel por parte do auditor, proporciona unha boa base para avaliar os controis relevantes relacionados coa información contable e financeira no nivel dos procesos de xestión.

b) Nivel de procesos/aplicacións de xestión

Os procesos de xestión (ou procesos de negocio) son os mecanismos que emprega unha entidade para desenvolver a súa actividade e prestar un servizo aos seus destinatarios ou usuarios.

Os CXTI a este nivel consisten nas políticas e procedementos establecidos para controlar determinados aspectos relacionados coa xestión da seguridade, controis de acceso lóxico, xestión da configuración e dos usuarios. *Por exemplo, os procedementos de xestión da configuración garantirán razoablemente que os cambios no software das aplicacións son verificados totalmente e están autorizados.*

Cando son examinados os CXTI a nivel de aplicación, o auditor financeiro e o auditor de sistemas avalían os controis de acceso lóxico que limitan ou restrinxen o acceso a determinadas aplicacións e ficheiros relacionados (como, por exemplo, o ficheiro mestre de empregados e os ficheiros de transaccións de nóminas) a usuarios autorizados baixo os principios de necesidade de saber e de mínimo privilexio.

Tamén se pode avaliar a seguridade establecida na propia aplicación para restrinxir o acceso en maior medida, normalmente mediante creación de usuarios con palabra clave de acceso e outras restricións programadas no software da aplicación mediante unha adecuada xestión dos perfís de usuario e os seus privilexios. Así, un empregado da función de nóminas pode ter acceso ás aplicacións sobre nóminas, pero pode ter restrinxido o acceso a unha determinada tarefa, como pode ser a revisión ou actualización de datos das nóminas sobre os empregados do propio departamento de nóminas ou sobre os datos do mestre de empregados.

[3] Committee of Sponsoring Organizations of the Treadway Commission

c) Nivel da infraestrutura TI

A infraestrutura TI constitúe a base das operacións da entidade e normalmente inclúen a xestión de redes e comunicacións, a xestión de bases de datos, a xestión de sistemas operativos, a xestión de almacenamento, a xestión das instalacións e os seus servizos e a administración de seguridade. Todo iso está xestionado por un departamento TI.

Os controis neste nivel están formados polos procesos que xestionan os recursos específicos do sistema TI relacionados co seu soporte xeral; son máis específicos que os establecidos ao nivel de entidade e normalmente están relacionados cun tipo determinado de tecnoloxía.

Dentro deste nivel hai varios subniveis ou capas tecnolóxicas que o auditor debe avaliar separadamente:

- ✓ Sistemas de xestión de bases de datos

  Os CXTI no nivel da base de datos fan fronte habitualmente aos riscos derivados da utilización das TI para realizar modificacións non autorizadas da información financeira das bases de datos mediante o acceso directo ás mesmas ou mediante a execución de scripts.

- ✓ Sistemas operativos (SO)

  É o software que controla a execución doutros programas de computador, programa tarefas, distribúe o almacenamento, xestiona as interfaces e mostra a interface por defecto co usuario cando non hai funcionando ningún outro programa.

  É moi importante realizar determinados procedementos de auditoría para analizar os controis existentes a este nivel, xa que vulnerabilidades nos SO teñen un impacto potencial en todo o sistema de información (aínda que as aplicacións e as bases de datos teñan bos controis, se un intruso puidese penetrar sen restricións no sistema operativo e o seu sistema de cartafoles, podería provocar graves danos nos datos e sistemas da entidade).

  Tamén se inclúe o middleware[4], os sistemas de virtualización, utilidades diversas, correo electrónico e aplicacións non relacionadas cos procesos de xestión da actividade da entidade.

- ✓ Sistemas de virtualización

  A tecnoloxía actual xeneralizou o uso de aplicacións que permiten crear "máquinas virtuais" para realizar as funcións de servidores de sistemas operativos e de soporte a outras aplicacións ou bases de datos e que melloran a eficiencia na xestión dos sistemas de información, permitindo aforros de espazo e de persoal significativos.

  O uso destas aplicacións atópase presente na maior parte dos sistemas de información actuais e representan un novo risco a considerar, xa que é frecuente que a maioría dos procesos críticos dunha entidade dependan do adecuado funcionamento da virtualización. Nestes casos será necesario revisar a súa adecuada configuración para garantir os controis do resto de sistemas dependentes.

- ✓ Redes

  Os CXTI a nivel de capa de rede cobren os riscos derivados do uso de técnicas de segmentación de rede, acceso remoto e autenticación. Os controis a este nivel son máis relevantes cando a entidade dispón de aplicacións web para procesos que xestionan información financeira. Tamén son importantes cando existen accesos ou intercambios de información con provedores ou existen servizos externalizados que requiren maior volume de transmisión de datos e/ou accesos remotos.

- ✓ Infraestrutura física

  Son todos os elementos físicos, o *hardware*. Inclúe as comunicacións.

[4] *Middleware* é software que permite a compatibilidade entre os distintos sistemas TI, SGBD e as aplicacións de negocio.

3.7 Os controis poden clasificarse en tres tipos:

Tipo	Características	Exemplos
Preventivo	A súa finalidade é previr que ocorra un feito que non é consistente cos obxectivos de control. Detecta os problemas antes de que sucedan. Monitoriza as operacións e os inputs e prevén erros, omisións ou actos malintencionados.	• Limitar o acceso aos sistemas TIC. Limitar o acceso mediante perfís de usuario e passwords a cambiar programas reduce o risco de transaccións non autorizadas.
Detectivo	Detectan e informan da ocorrencia dun erro, omisión ou acto malintencionado.	• Un supervisor revisa semanalmente todos os pases a produción das modificacións nas aplicacións para verificar que están debidamente autorizadas.
Compensatorio	Se é efectivo, pode limitar ou mitigar a gravidade dunha deficiencia de control interno. Limitan a gravidade dunha deficiencia e as súas consecuencias, pero non a eliminan.	• En entidades de reducida dimensión os controis de segregación de funcións poden ser difíciles de implantar e deben compensarse con controis que impliquen unha maior supervisión ou control xerencial.

Figura 3

4. Interrelación dos controis xerais cos controis de aplicación

4.1 Os CXTI axudan a asegurar o correcto funcionamento dos sistemas de información mediante a creación dunha contorna adecuada para o correcto funcionamento dos controis de aplicación.

Unha avaliación favorable dos CXTI dá confianza ao auditor sobre os controis de aplicación automatizados integrados nas aplicacións de xestión. Se non existisen controis xerais ou non fosen efectivos, non se podería confiar nos controis de aplicación e sería necesario adoptar un enfoque de auditoría baseado exclusivamente en procedementos substantivos. É dicir, a eficacia dos CXTI afecta á estratexia de auditoría que se debe adoptar.

Para máis detalles ver apartado 5 na FGPF-OCEX 5340.

5. Categorías de controis xerais

5.1 Existen diversas clasificacións de CXTI segundo o marco conceptual[5] que se adopte e de cales sexan os obxectivos da auditoría, aínda que as subcategorías e controis son basicamente coincidentes en todos os casos. Para os efectos desta guía, os CXTI agrupáronse en cinco categorías, de acordo co esquema básico mostrado na Figura 4.

[5] Por exemplo: INTOSAI/WIGITA, COBIT, FISCAM da GAO, NIA-ES 315.

Categorías de controis	Controis principais	Medidas do ENS
A. Marco organizativo	A.1 Cumprimento de legalidade (CBCS.8)	org.1
	A.2 Estratexia de seguridade	org.2
	A.3 Organización e persoal de TI	
	A.4 Marco normativo e procedimental de seguridade	mp.per
B. Xestión de cambios en aplicacións e sistemas	B.1 Adquisición de aplicacións e sistemas	
	B.2 Desenvolvemento de aplicacións	mp.sw.1 e 2
	B.3 Xestión de cambios	op.exp.5
C. Operacións dos sistemas de información	C.1 Inventario de hardware e software (CBCS 1 e 2)	op.exp.1
	C.2 Xestión de vulnerabilidades (CBCS.3)	op.exp.3 e 4
	C.3 Configuracións seguras (CBCS.5)	op.exp.2 e 3
	C.4 Rexistro da actividade dos usuarios (CBCS.6)	op.exp.8 e 10
	C.5 Servizos externos	op.ext.1 e 2
	C.6 Protección fronte a malware	op.exp.6
	C.7 Protección das instalacións e infraestruturas	mp.if
	C.8 Xestión de incidentes	op.exp.7 e 9
	C.9 Monitorización	
D. Controis de acceso a datos e programas	D.1 Uso controlado de privilexios administrativos (CBCS.4)	op.acc.4
	D.2 Mecanismos de identificación e autenticación	op.acc.1 e 5
	D.3 Xestión de dereitos de acceso	op.acc.4
	D.4 Xestión de usuarios	op.acc
	D.5 Protección das redes e comunicacións	mp.com
E. Continuidade do servizo	E.1 Copias de seguridade de datos e sistemas (CBCS.7)	mp.info.9
	E.2 Plan de continuidade	op.cont.2 e 3
	E.3 Alta dispoñibilidade	mp.if.9

Códigos de cores: Controis básicos de ciberseguridade (*son controis mínimos a revisar en calquera fiscalización*)

Figura 4

5.2 A ausencia dunha actividade de control determinada ou a ineficacia do seu deseño, non significa que o sistema de control interno dunha entidade teña un deseño inadecuado, xa que en moitos casos o risco provocado por aquela deficiencia pode ser mitigado por un control compensatorio. Situacións deste tipo preséntanse con frecuencia nas organizacións pequenas.

6. Identificar que CXTI son relevantes para revisar nunha auditoría

6.1 Nunha entidade mediana ou grande pódense identificar, en conxunto, numerosos CXTI que:

- Resulta materialmente imposible revisalos na súa totalidade.
- Gran parte deles non teñen interese para os obxectivos da auditoría.
- Só un pequeno subconxunto ten impacto no risco de auditoría.

A estes últimos denominarémolos controis relevantes e neles deberá centrar a atención e traballo o auditor. Para iso aplicarase a metodoloxía descrita no anexo 2 da GPF-OCEX 1315, segundo a cal a análise das contas a auditar conduce a identificar as aplicacións de xestión significativas nas que debe centrar o esforzo o auditor.

A continuación, o enfoque de risco require que para cada área ou aplicación significativa:

- Se valoren os RIM relacionados.
- Se revise a eficacia do control interno:
  1º os CXTI relacionados, e
  2º os controis de procesos /aplicación de xestión
- Se realicen as probas substantivas.

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

6.2 Debido ao gran número de CXTI que existen nunha entidade mediana ou grande, o enfoque de risco brevemente descrito permítenos centrarnos 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, o resto carece de interese para a auditoría financeira.

Se o número de aplicacións significativas é elevado, tal como sucede por exemplo na auditoría das contas dunha comunidade autónoma, será imposible revisar todos os controis de aplicación e CXTI relacionados. Nestes casos deberase establecer un plan de auditoría plurianual que estableza un calendario para a revisión dos controis automatizados, tanto de aplicación como xerais, que sexa realizable cos recursos do OCEX.

Se se revisan os CXTI 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 inmobilizado, tampouco se revisarían os controis de acceso ou a xestión de usuarios da aplicación de ingresos, xa que eses traballos non nos permitirían reducir o risco de auditoría da área de gastos de persoal. Deberíanse revisar os CXTI 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.

É dicir, os CXTI deben avaliarse en relación co seu efecto nas aplicacións significativas e nos datos relacionados coas contas anuais auditadas. *Por exemplo, se non se implementaron novos sistemas durante o período auditado, as debilidades nos CXTI sobre o desenvolvemento de sistemas poden non ser relevantes respecto das contas anuais auditadas.*

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

Pero se a auditoría dos sistemas de información forma parte dunha auditoría financeira (ou dunha auditoría operativa) **analizarase cos auditores financeiros** aqueles controis que son relevantes para os obxectivos da auditoría financeira (ou operativa), xa que non todos os riscos son iguais, nin en probabilidade, nin na súa materialidade. Deberase adoptar un enfoque baseado na análise do risco.

Por outra banda, todos os controis tampouco son iguais no seu grao de eficacia á hora de reducir os riscos identificados; por tanto non será necesario avaliar todas as actividades de control relacionadas cun risco concreto, hai que cinguirse unicamente a aqueles controis que sexan relevantes, é dicir, aqueles que proporcionan unha maior seguridade de que o obxectivo de control acadouse.

Un control será relevante cando a súa ausencia ou o seu mal funcionamento representa unha deficiencia significativa ou unha debilidade material de control interno. Noutras palabras é aquel que proporciona unha seguridade razoable de que incorreccións materiais serán previdas ou detectadas

oportunamente. En consecuencia, o auditor seleccionará para revisar só os controis relevantes, é dicir aqueles que lle permitan mitigar determinados riscos de incorrección material.

6.4 Á hora de decidir se un control é relevante, debe aplicarse o xuízo profesional, e terase en conta o seguinte:

- Os controis relevantes xeralmente inclúen políticas, procedementos, prácticas e unha estrutura organizativa que son esenciais para que a dirección poida reducir os riscos significativos e alcanzar o obxectivo de control relacionado.
- Os controis relevantes a miúdo apoian máis dun obxectivo de control.

  Por exemplo, os controis de acceso apoian a integridade e validez das transaccións financeiras, as valoracións contables, a segregación de tarefas, etc.

  Na maioría dos casos, resulta efectivo facer unha combinación de controis relevantes a fin de alcanzar un obxectivo concreto ou ben unha serie de obxectivos, para non depender demasiado dun só control.
- Os controis que fan fronte directamente aos riscos significativos son con frecuencia relevantes.

  Por exemplo, o risco de acceso non autorizado é un risco significativo para a maioría de entidades; por tanto, os controis de seguridade que preveñen ou detectan accesos non autorizados son importantes.
- Os controis preventivos son por regra xeral máis eficientes que os detectivos. Por tanto, os controis preventivos considéranse a miúdo relevantes.

  Por exemplo, previr que se produza unha fraude é moito mellor que simplemente detectalo despois de que ocorrese.
- Os controis automatizados son máis fiables que os controis manuais.

  Por exemplo, os controis automatizados que obrigan ao usuario para cambiar periodicamente de contrasinal son máis fiables que as normas xenéricas que non son de uso forzoso. Os procesos manuais tamén están expostos a erros humanos.

6.5 Para cada CXTI que se identificou como relevante, o auditor debe aplicar **procedementos** para **analizar a efectividade do seu deseño para realizar a actividade de control**, considerando o risco TI e os obxectivos da auditoría.

Se se conclúe que o deseño é eficaz aplicaranse procedementos de auditoría para **verificar se está implementado e en funcionamento durante todo o período auditado**.

7. Procedementos de auditoría

7.1 O primeiro paso, en calquera auditoría, é obter un coñecemento adecuado do que se vai a auditar, neste caso do sistema de información e dos controis xerais.

Os procedementos de auditoría a executar para coñecer a contorna tecnolóxica e os CXTI dependerán do tipo de auditoría que se vaia a realizar, dos obxectivos da mesma e da profundidade requirida.

7.2 Terase unha reunión na que se explicará persoalmente ao responsable de TI e ao coordinador cal é o obxectivo xeral do traballo, calendario e información que se lles vai a solicitar.

A solicitude da información poderá realizarse por escrito ou correo electrónico dirixido ao coordinador da fiscalización ou ao responsable do departamento de TI (se se acorda este procedemento co coordinador e o responsable de TI) ao iniciarse a fiscalización.

O equipo de auditoría debe asegurar a seguridade no envío e recepción da información sobre os sistemas de información do ente auditado xa que, en xeral, trátase de información confidencial que podería ser utilizada por persoas mal intencionadas para vulnerar os sistemas de información auditados.

Toda a información sensible en tránsito (computadores portátiles, lapis de memoria ou a través de internet) deber estar cifrada.

7.3 Sen ánimo de ser exhaustivo poden presentarse as seguintes situacións:

a) Auditorías operativas ou específicas de sistemas de información:

- Auditorías dos controis de ciberseguridade.
- Auditoría de sistemas dos rexistros contables de facturas.
- Auditoría dos sistemas de control interno.
- Auditoría de seguridade.
- Etc.

Nestas auditorías requiriranse procedementos especificamente deseñados, que normalmente incluirán ou estarán baseados no cuestionario do Anexo 3 e o traballo documentarase nas fichas do Anexo 4.

b) Auditoría de sistemas de información en apoio de auditorías financeiras ou de cumprimento.

- Auditorías con alcances limitados.

  En calquera auditoría que requira un coñecemento básico da entidade e do seu sistema de control interno, revisaranse os CBCS (véxase a GPF-OCEX 5313), que están incluídos no programa do Anexo 4.

- 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.

  Nestas auditorías xunto coa petición inicial de información solicitarase que se cumprimente o cuestionario do Anexo 3 (axustado ao alcance de controis que se determine), obteranse evidencias adicionais e documentarase o traballo realizado e as conclusións coas fichas do Anexo 4.

  Os CBCS terán carácter de revisión mínima e están incluídos no programa do Anexo 4.

  Os controis para revisar serán os do apartado 5.

7.4 No Anexo 2 achégase un modelo de programa xeral para incluír nos programas de traballo das auditorías financeiras.

7.5 O cuestionario que se achega como Anexo 3 está deseñado para:

- Obter información xeral sobre os sistemas de información da entidade fiscalizada e dos CXTI.
- Axudar a identificar a existencia de deficiencias neses controis que poidan derivar en riscos significativos de auditoría.

O cuestionario estrutúrase nas 5 áreas vistas no apartado cinco.

7.6 Tras recibir o cuestionario cumprimentado, o equipo de auditoría analizará a información contida no mesmo, que se utilizará para realizar o traballo previsto no Anexo 4.

Estas fichas están deseñadas para:

- Axudar a obter información avanzada sobre os sistemas de información da entidade fiscalizada e dos CXTI.
- Axudar a identificar actividades e obxectivos de control relacionadas cos CXTI.
- Axudar a avaliar o deseño e eficacia dos CXTI da entidade auditada.

- Axudar a identificar a existencia de deficiencias neses controis que poidan derivar en riscos significativos de auditoría.
- **Documentar** os procedementos levados a cabo, a evidencia obtida e as conclusións alcanzadas respecto á eficacia e implementación dos CXTI.

Estas fichas/programa estándar debe adaptarse en cada caso ás características do ente auditado, dos seus sistemas de información, e do obxectivo e alcance da auditoría. Os obxectivos de control son invariables, pero o deseño dos controis e as características da súa implementación son específicos de cada entidade.

Estes procedementos executaranse naquelas fiscalizacións na que se deba emitir unha opinión de auditoría de seguridade razoable sobre as contas anuais ou un compoñente significativo das mesmas en entidades na que a súa actividade se apoie en sistemas TIC ou naquelas auditorías específicas dos CXTI.

Este procedemento foi deseñado para ser completado por persoal con coñecementos sobre os CXTI. En xeral realizarase por un especialista en auditoría de sistemas de información.

As fichas estrutúranse nas 5 áreas vistas no apartado cinco.

7.7 Unha vez cumprimentado o Anexo 4, **concluirase** indicando:

- Conclusións xerais sobre os controis revisados.
- Identificar e evidenciar as deficiencias de control detectadas.
- Identificar e documentar riscos incorrección material sobre os estados financeiros.
- Necesidade de traballo adicional.

7.8 A información obtida, as evidencias e as conclusións sobre as mesmas documentaranse no arquivo de papeis de traballo electrónicos creado para a fiscalización dentro dunha área específica para a revisión dos sistemas de información.

8. Avaliación das deficiencias de control interno detectadas

8.1 Cada un dos controis principais sinalados na Figura 4 está composto por unha serie de **subcontrois ou controis detallados**, que son detallados nas fichas de revisión do Anexo 4. Nestas fichas débese documentar o traballo realizado e concluír para cada subcontrol, en base ás evidencias, sobre a súa **eficacia** podendo atoparse cada un deles nalgunha das seguintes situacións:

	Control efectivo
	Control bastante efectivo
	Control pouco efectivo
	Control non efectivo

8.2 Ademais cada **control principal** (composto por subcontrois) avaliarase utilizando o modelo de **nivel de madurez** (ver Anexo 1) e deberase concluír nas mesmas FICHAS DE REVISIÓN. Para avaliar o nivel de madurez terase en conta os resultados obtidos nos subcontrois que o forman e a importancia relativa destes para o cumprimento do obxectivo de control.

8.3 Tras analizar os resultados da revisión de cada control extraeranse as deficiencias de control interno observadas e as recomendacións que se deriven das mesmas, que deben estar ben soportadas nos papeis de traballo. Os achados de auditoría que as soportan deben incluír: *(GPF-OCEX 1735; P9)*

Criterio (de auditoría): a referencia ou norma coa que se compara ou avalía o feito observado; o que debería ser.

Nas auditorías de sistemas de información (CXTI, controis de aplicación e cibercontrois) os criterios de auditorías son os establecidos con carácter xeral na GPF-OCEX relacionadas, que están baseadas no ENS, NIA-ES, ISSAI, etc.

Feito ou condición: a situación observada e documentada na auditoría.

Están baseados en evidencia de auditoría. Poden ser deficiencias de control, problemas operacionais ou incumprimento de requirimentos legais ou administrativos.

Causa: as razóns que dan lugar ao feito observado.

Pode servir como base para propoñer accións correctoras nas recomendacións. Débese identificar a unidade ou departamento responsable da deficiencia.

As causas máis comúns inclúen políticas, procedementos ou criterios mal deseñados, ou aplicados de forma inconsistente, incompleta ou incorrecta; ou factores máis aló do control dos xestores. Os auditores poden avaliar se a evidencia proporciona un argumento razoable e convincente de por que a causa indicada é o factor clave que contribúe á diferenza entre a condición e os criterios.

Efecto: que consecuencia negativa ten lugar ou podería ter lugar, provocada pola diferenza entre o feito observado e o criterio.

Explica o impacto adverso ao obxectivo operacional ou obxectivo do control. Ao articular o impacto e o risco, o elemento do efecto real ou potencial é moi importante para axudar a convencer á administración do auditado da necesidade de tomar accións correctoras en resposta aos problemas e/ou riscos significativos identificados.

Recomendación: accións correctoras suxeridas.

As recomendacións deben redactarse de forma que se aborde a corrección das causas que orixinan o feito ou condición observado.

8.4 Ao avaliar as deficiencias de control interno detectadas débense considerar a **significatividade** destas. Neste contexto o concepto "significativo" non pode ser definido de forma exacta, xa que unha mesma cuestión pode ser significativa, ou non, dependendo dos obxectivos da auditoría e das circunstancias. *(GPF-OCEX 1735; P10)*

8.5 As deficiencias de control interno clasifícanse en tres niveis de importancia relativa ao examinar o control interno: *(GPF-OCEX 1735; P11)*

- Unha **deficiencia de control interno** existe cando o deseño ou o funcionamento dun control non permite ao persoal da entidade ou á súa dirección, no curso ordinario das operacións, previr ou detectar erros ou irregularidades nun prazo razoable. Poden ser *deficiencia de deseño* do control (cando un control necesario para alcanzar o obxectivo de control non existe ou non está adecuadamente deseñado) ou *deficiencias de funcionamento* (cando un control adecuadamente deseñado non opera tal como foi deseñado ou a persoa que o executa non o realiza eficazmente).
- Unha **deficiencia significativa** é unha deficiencia no control interno, ou unha combinación de deficiencias, que afectan adversamente a capacidade da entidade para iniciar, autorizar, rexistrar, procesar ou reportar información financeira ou orzamentaria de forma fiable, de conformidade cos principios ou normas contables e/ou orzamentarias aplicables, e existe unha probabilidade que é máis que remota, de que unha manifestación errónea nas contas anuais, ou un incumprimento, que non é claramente trivial, non sexa previda ou detectada en prazo oportuno.
- Unha **debilidade material** é unha deficiencia significativa no control interno ou unha combinación delas, respecto das que existe unha razoable posibilidade de que unha manifestación errónea significativa nas contas anuais ou un incumprimento de carácter grave non sexa previda ou detectada e corrixida en prazo oportuno.

8.6 A avaliación de importancia relativa ou significatividade das deficiencias inclúe consideracións sobre os seguintes factores de carácter xeral: a magnitude do impacto, a probabilidade de que ocorra e a natureza da deficiencia. *(GPF-OCEX 1735; P12)*

Implica avaliar, no contexto dos obxectivos da auditoría, os seguintes factores:

a) A magnitude do impacto refírese para o efecto probable que a deficiencia puidese ter no logro dos obxectivos da entidade e vese afectado por factores como o tamaño, o ritmo e a duración do impacto da deficiencia. Unha deficiencia pode ser máis significativa para un obxectivo que para outro.

b) A probabilidade de ocorrencia refírese á posibilidade de que unha deficiencia afecte á capacidade dunha entidade para alcanzar os seus obxectivos.

c) A natureza da deficiencia implica factores tales como o grao de subxectividade implicado coa deficiencia e se a deficiencia xorde da fraude ou dunha conduta indebida.

8.7 En particular, para determinar se unha deficiencia de control, individualmente ou xunto con outras, constitúe unha deficiencia significativa ou unha debilidade material, o auditor pode considerar, entre outros, os seguintes factores:

- Prexudica ou pode prexudicar o cumprimento dos obxectivos da entidade.
- É unha deficiencia de control interno que ocasiona un aumento significativo do risco de auditoría.
- A probabilidade de que unha persoa poida obter acceso non autorizado ou executar actividades non autorizadas ou inapropiadas en sistemas críticos da entidade ou arquivos que poidan afectar á información con impacto nas contas anuais. Isto pode incluír:

  (1) a habilidade para ter acceso a sistemas nos que residen aplicacións críticas e que posibilita a usuarios non autorizados a ler, engadir, borrar, modificar ou extraer información financeira, ben directamente ou a través da utilización de software non autorizado;
  (2) a habilidade para acceder directamente e modificar ficheiros que conteñan información financeira; ou
  (3) a habilidade para asignar dereitos de acceso ás aplicacións a usuarios non autorizados, coa finalidade de procesar transaccións non autorizadas.

- A natureza dos accesos non autorizados que poden conseguirse (por exemplo: limitados a programadores do sistema ou das aplicacións ou a administradores do sistema; a todos os usuarios; a alguén externo a través de acceso non autorizados por Internet) ou a natureza das actividades non autorizadas ou inadecuadas que poden levarse a cabo.
- A probabilidade de que importes das contas anuais estean afectados de forma significativa.
- A probabilidade de que outros controis poidan previr ou detectar accesos non autorizados.
- O risco de que a dirección da entidade poida burlar os controis (por exemplo, mediante dereitos de acceso excesivos).

8.8 Ademais ao avaliar as deficiencias dun CXTI deben facerse outras consideracións adicionais:

- **Efecto nos controis das aplicacións**.

  A importancia dunha deficiencia nun CXTI debe ser avaliada en relación co seu efecto nos controis de aplicación, é dicir, se provoca que os controis de aplicación sexan ineficaces. Se a deficiencia da aplicación é provocada polo CXTI ambas deficiencias deben ser consideradas da mesma forma (como deficiencias significativas ou como debilidades materiais).

- **Efecto na contorna de control**.

  Despois de que unha deficiencia dun CXTI fose avaliada en relación cos controis de aplicación, tamén debe ser avaliada considerando o conxunto das deficiencias de control e o seu efecto agregado. Por exemplo debe considerarse a decisión da xerencia de non emendar unha deficiencia de CXTI e reflexionar sobre a súa relación coa contorna de control; ao considerala agregada a outras deficiencias que afectan a contorna de control pode levar á conclusión de que existe unha debilidade material ou unha deficiencia significativa na contorna de control.

- **Análise do efecto agregado das deficiencias de control.**

  Algunhas deficiencias de control poden ser consideradas non significativas individualmente, pero consideradas conxuntamente con outras deficiencias similares, o efecto combinado pode ser máis significativo. Por exemplo, nunha entidade que non realiza revisións periódicas das listas de usuarios con acceso á súa aplicación de contabilidade considerarase que ten unha deficiencia no deseño dun control. Por unha banda poida que non se considere significativa, especialmente se existen controis compensatorios. Pero se se detectou que o procedemento de autorización de novos usuarios a esa aplicación é inadecuado, entón o efecto agregado das dúas deficiencias pode resultar nunha deficiencia significativa ou nunha debilidade material. É dicir, o efecto combinado das deficiencias de control relacionadas coas solicitudes de novos accesos e as revisións dos dereitos de acceso nunha aplicación contable, cuestiona a validez dos permisos de acceso nesa aplicación e en consecuencia expón dúbidas sobre a validez das transaccións dentro do sistema de información.

8.9 Baseándose nas consideracións apuntadas o auditor financeiro e o auditor informático, conxuntamente, determinarán se as deficiencias de control son, individualmente ou en conxunto, debilidades materiais ou deficiencias significativas.

Se as deficiencias de control constitúen debilidades materiais, o auditor concluirá que os CXTI non son eficaces e deberá reformularse a súa estratexia de auditoría, omitindo revisar os controis de aplicación debido a que non van ser eficaces, dando maior énfase aos procedementos substantivos, de forma que se tentará minimizar o risco final de auditoría.

8.10 Se se efectúan **recomendacións**, existirá unha relación directa entre o tipo de deficiencia de control (segundo a súa importancia relativa), o risco de auditoría que representa, e a prioridade que se conceda a cada recomendación.

A prioridade tamén estará matizada por consideracións custo/beneficio.

No cadro seguinte resúmese a relación existente entre os tres tipos de deficiencias de control segundo a súa significatividade ou importancia relativa, o risco que representan e a prioridade das recomendacións correspondentes: *(GPF-OCEX 1735; P13)*

Tipo de deficiencia segundo a súa importancia relativa	Risco	Prioridade dunha recomendación	
Debilidade material	**Alto**	**Alta**	**Requírese atención urxente da dirección para implantar controis/procedementos que mitiguen os riscos identificados.**
Deficiencia significativa	**Medio**	**Media**	**A dirección debería establecer un plan de acción concreto para resolver a deficiencia observada nun prazo razoable.**
Deficiencia de control interno	**Baixo**	**Baixa**	

Figura 6

8.11 **As debilidades materiais deben ser incluídas no informe de auditoría como unha excepción ou como unha conclusión, segundo o tipo de informe**.

Anexo 1. Niveis de madurez dos procesos segundo a Guía de seguridade CCN-STIC 804

Para avaliar os resultados xerais por cada un dos CXTI utilizarase o modelo de nivel de madurez dos procesos[6] usando unha escala entre 0 e 5. Este modelo proporciona unha base para comparar resultados entre distintos entes e entre distintos períodos para un ente determinado.

Nivel	Descrición
0 - Inexistente.	Esta medida non está a ser aplicada neste momento.
1 - Inicial / ad hoc	O proceso existe, pero non se xestiona. O enfoque xeral de xestión non é organizado. *A organización non proporciona unha contorna estable. O éxito ou fracaso do proceso depende da competencia e boa vontade das persoas e é difícil prever a reacción ante unha situación de emerxencia. Neste caso, as organizacións exceden con frecuencia orzamentos e tempos de resposta. O éxito do nivel 1 depende de ter persoal de alta calidade.*
2 - Repetible, pero intuitivo.	Os procesos seguen unha pauta regular cando determinados procedementos realízanse por distintas persoas, sen procedementos escritos nin actividades formativas. *A eficacia do proceso depende da boa sorte e da boa vontade das persoas. Existe un mínimo de planificación que proporciona unha pauta para seguir cando se repiten as mesmas circunstancias. É impredicible o resultado se se dan circunstancias novas. Aínda hai un risco significativo de exceder as estimacións de custo e tempo.*
3 - Proceso definido	Os procesos están estandarizados, documentados e comunicados con accións formativas. *Disponse un catálogo de procesos que se mantén actualizado. Estes procesos garanten a consistencia das actuacións entre as diferentes partes da organización, que adaptan os seus procesos particulares ao proceso xeral. Hai normativa establecida e procedementos para garantir a reacción profesional ante os incidentes. Exércese un mantemento regular. As oportunidades de sobrevivir son altas, aínda que sempre queda o factor do descoñecido (ou non planificado). O éxito é algo máis que boa sorte: merécese.* *Unha diferenza importante entre o nivel 2 e o nivel 3 é a coordinación entre departamentos e proxectos, coordinación que non existe no nivel 2, e que se xestiona no nivel 3.*
4 - Xestionado e medible.	A Dirección controla e mide o cumprimento cos procedementos e adopta medidas correctoras cando se require. *Disponse dun sistema de medidas e métricas para coñecer o desempeño (eficacia e eficiencia) dos procesos. A Dirección é capaz de establecer obxectivos cualitativos a alcanzar e dispón de medios para valorar se se alcanzaron os obxectivos e en que medida.* *No nivel 4 de madurez, o funcionamento dos procesos está baixo control con técnicas estatísticas e cuantitativas. A confianza está cuantificada, mentres que no nivel 3, a confianza era soamente cualitativa.*
5 - Optimizado.	Séguense boas prácticas nun ciclo de mellora continua. *O nivel 5 de madurez céntrase na mellora continua dos procesos con melloras tecnolóxicas incrementais e innovadoras. Establécense obxectivos cuantitativos de mellora. E revísanse continuamente para reflectir os cambios nos obxectivos de negocio, utilizándose como indicadores na xestión da mellora dos procesos.* *Neste nivel a organización é capaz de mellorar o desempeño dos sistemas a base dunha mellora continua dos procesos baseada nos resultados das medidas e indicadores.*

[6] Baseado na Guía de seguridade CCN-STIC 804.