1. Introdución

Na *GPF-OCEX 5311 Ciberseguridade, seguridade da información e auditoría externa*, destácase a importancia crecente que as cuestións relacionadas coa ciberseguridade están a adquirir na xestión das administracións públicas e, en consecuencia, a atención crecente que os auditores públicos deben conceder a dita materia. Na medida en que cada vez un maior número de servizos públicos préstase on-line e a conectividade por internet converteuse nunha característica de todos os sistemas de información (contables, sanitarios, educativos, etc) os auditores deben prestar cada vez máis atención ás cuestións relacionadas coa ciberseguridade.

Tamén se mencionan na citada guía os distintos enfoques que os OCEX poden adoptar á hora de abordar unha auditoría ou unha revisión da ciberseguridade dos entes públicos. En síntese, desde a perspectiva dun OCEX, pódense adoptar tres enfoques principais:

- Realizar unha auditoría de ciberseguridade consistente nunha análise a fondo da cuestión nun determinado ente.

  Podería ser similar a unha auditoría de seguridade das requiridas polo ENS[1] ou unha auditoría seguindo a metodoloxía de ISACA[2]. Un traballo deste tipo entraña unha intensa dedicación de persoal especializado tanto para o auditor como para o ente auditado.

- A revisión de aspectos directamente relacionados coas áreas significativas nunha auditoría financeira.

  Consistirá na revisión dos Controis Xerais de Tecnoloxías da Información (CXTI) relacionados unicamente coas áreas significativas para os fins da auditoría financeira do ente auditado. Unha parte significativa de ditos controis está formada por controis de ciberseguridade. Este é o obxecto da GPF-OCEX 5330.

- A revisión dunha serie de controis básicos de ciberseguridade.

  Os controis básicos de ciberseguridade son un subconxunto reducido dos controis de ciberseguridade. A súa revisión permitirá formar unha idea xeral da situación na entidade revisada e non requirirá a dedicación de excesivos recursos especializados nin do auditor externo nin do ente auditado. Será por tanto un traballo máis viable en entes que non dispoñan de moitos recursos técnicos ou humanos.

  Un enfoque deste tipo é o que motiva o desenvolvemento da presente guía.

---

1 Seguindo por exemplo as guías CCN-STIC-802, 808 e 804.

2 Na bibliografía final cítanse dúas guías de ISACA que poderían utilizarse para este propósito.

2. Os Controis Básicos de Ciberseguridade (CBCS)

No desenvolvemento desta GPF-OCEX 5313, cuxo contido está fundamentalmente relacionado coa auditoría da seguridade da información, tívose especial coidado en manter a máxima coherencia cos postulados do ENS debido a que é de obrigado cumprimento para todos os entes públicos e esta aliñación facilita a realización das auditorías de ciberseguridade e coadxuvan á implantación do ENS. Con todo, dada a súa amplitude, seleccionáronse, polas razóns sinaladas no apartado anterior, unha serie limitada de controis para a súa revisión. Con obxecto de seleccionar os máis relevantes atendeuse ao marco conceptual establecido polo Center for Internet Security[3] (CIS) que prioriza e clasifica os controis segundo a súa importancia para facer fronte ás ciberamenazas.[4]

Tal como se sinala no anexo 4 da GPF-OCEX 5311, os controis de seguridade críticos do CIS son un conxunto conciso e **priorizado** de accións de ciberdefensa, orientados a mitigar os ataques máis comúns e daniños coa intención de automatizalos o máximo posible. Inclúen 20 controis de seguridade da información aliñados coa publicación NIST[5] 800-53. En agosto de 2016 publicouse a versión 6.1, e en 2018 actualizáronse á versión 7 e cambiouse a súa denominación a **Controis CIS**. Estes controis están pensados para organizacións de calquera tipo.

Segundo o CIS[6], con carácter xeral, as organizacións que apliquen só os cinco primeiros controis poden reducir o seu risco ante ciberataques ao redor do 85%. Se se implementan os 20 controis o risco pódese reducir un 94%. A nova versión 7 clasifica os 6 primeiros controis como **Básicos** e son os que se utilizaron como referencia nesta guía para establecer os controis básicos de ciberseguridade (CBCS) dos OCEX.

Ademais dos seis controles CIS básicos incluíuse nos CBCS o control "Copias de seguridade de datos e sistemas" (control CIS número 10) xa que é un elemento fundamental para manter un grao razoable de ciber-resiliencia[7]. Se todos os controis preventivos fallan e un ciberataque traspasa todas as liñas de defensa e ten éxito, o último recurso da entidade atacada é restaurar os seus sistemas e datos nun prazo predeterminado para poder continuar prestando os seus servizos.

[3] Organización de recoñecido prestixio internacional.

[4] Non é o único marco de ciberseguridade que establece unha priorización de controis, pero si é un dos máis recoñecidos internacionalmente. Son varios os países que estableceron listas priorizadas de medidas de ciberseguridade, por exemplo, a Australian National Audit Office no seu recente informe Cyber Resilience establece como criterio de auditoría as estratexias de mitigación das ciberamenazas denominadas Essential Eight, que deben aplicar as entidades públicas dese país.

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

[6] Guide to the First 5 CIS Controls (v6.1).

[7] Ciber-resiliencia é a capacidade para continuar prestando servizos mentres se preveñen e responden os ciberataques. Tamén reduce a probabilidade de que os ciberataques teñan éxito. Para ser ciber-resiliente, unha entidade pública debe ter implementado un sólido sistema de CXTI, cuxa función é proporcionar unha contorna TI fiable sobre o que outros procesos e controis TI poden apoiarse e funcionar.

Os sete controles básicos de ciberseguridade debidamente referenciados co ENS son:

Control		Obxectivo de control	Medidas de seguridade do ENS
CBCS 1	Inventario e control de dispositivos físicos	Xestionar activamente todos os dispositivos hardware na rede, de forma que só os dispositivos autorizados teñan acceso á rede.	op.exp.1
CBCS 2	Inventario e control de software autorizado e non autorizado	Xestionar activamente todo o software nos sistemas, de forma que só se poida instalar e executar software autorizado.	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación e remediación de vulnerabilidades	Dispoñer dun proceso continuo para obter información sobre novas vulnerabilidades, identificalas, remedialas e reducir a xanela de oportunidade aos atacantes.	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilexios administrativos	Desenvolver procesos e utilizar ferramentas para identificar, controlar, previr e corrixir o uso e configuración de privilexios administrativos en computadores, redes e aplicacións.	op.acc.4 op.acc.5
CBCS 5	Configuracións seguras do software e hardware de dispositivos móbiles, portátiles, equipos de sobremesa e servidores	Implementar a configuración de seguridade de dispositivos móbiles, portátiles, equipos de sobremesa e servidores, e xestionala activamente utilizando un proceso de xestión de cambios e configuracións rigoroso, para previr que os atacantes exploten servizos e configuracións vulnerables.	op.exp.2 op.exp.3
CBCS 6	Rexistro da actividade dos usuarios	Recoller, xestionar e analizar logs de eventos que poden axudar a detectar, entender ou recuperarse dun ataque.	op.exp.8 op.exp.10
CBCS 7	Copias de seguridade de datos e sistemas	Utilizar procesos e ferramentas para realizar a copia de seguridade da información crítica cunha metodoloxía probada que permita a recuperación da información en tempo oportuno.	mp.info.9

Figura 1

Sen dúbida unha auditoría dos 20 controis CIS ou unha auditoría seguindo o ENS[8], proporcionará unha maior seguridade sobre a situación do ente auditado fronte ás ciberameazas e o seu nivel de ciber-resiliencia. Pero, como xa se sinalou, o esforzo requirido na execución de traballos con ese amplo alcance limita a súa aplicación na práctica.

Por esta razón e debido a que os CBCS están priorizados, de máis efectivos a menos, unha alternativa con mellor relación custo/beneficio consiste en deseñar un plan de traballo baseado nos sete controles básicos de ciberseguridade máis os controis de legalidade do seguinte apartado, criterio que recolle esta guía [9].

[8] De acordo coa *Guía de auditoría do ENS CCN-STIC-802.*

[9] Os Controis CIS xa se usaron como criterios de auditoría de referencia en auditorías de ciberseguridade realizadas por auditores públicos de prestixio recoñecido. 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*.

3. Revisión de cumprimento da legalidade

Ademais dos CBCS vistos no apartado anterior, neste tipo de revisión incluirase a verificación do cumprimento de diversas normas relacionadas coa seguridade da información:

Control de legalidade		Obxectivo de cumprimento	Medidas de seguridade do ENS
CBCS 8	Cumprimento do ENS	• Política de seguridade e responsabilidades • Declaración de aplicabilidade • Informe de Auditoría (nivel medio ou alto) • Informe do estado da seguridade • Publicación da declaración de conformidade e os distintivos de seguridade na sede electrónica	Org1 Art 27.4 Art.34 Art.35 Art.41
	Cumprimento da LOPD/RGPD	• Nomeamento do DPD • Rexistro de actividades de tratamento • Análise de riscos e avaliación do impacto das operacións de tratamento *(para os de risco alto)* • Informe de auditoría de cumprimento *(cando o responsable do tratamento decidise realizala)*	--
	Cumprimento da Lei 25/2013, do 27 de decembro *(Impulso da factura electrónica e creación do rexistro contable de facturas)*	• Informe de auditoría de sistemas anual[10] do Rexistro Contable de Facturas	--

Figura 2

4. Obxectivos da auditoría dos CBCS

O obxectivo da auditoría é proporcionar unha avaliación sobre o deseño e a eficacia operativa dos controis básicos de ciberseguridade mediante:

- A identificación de deficiencias de control interno que poidan afectar negativamente á integridade, dispoñibilidade, autenticidade, confidencialidade e trazabilidade dos datos, a información e os activos da entidade.
- A identificación de incumprimentos normativos relacionados coa ciberseguridade.

Dado o carácter limitado da revisión, o obxectivo non é emitir unha opinión de seguridade razoable sobre a confianza que merece o sistema auditado en relación co nivel de ciberseguridade implantado. Con todo, a auditoría proporcionará información relevante sobre o grao de ciberseguridade e ciber-resiliencia da entidade e sobre posibles accións de mellora aconsellables.

[10] De acordo ao esixido na Lei 25/2013, do 27 de decembro, de impulso da factura electrónica e creación do rexistro contable de facturas no Sector Público *(Artigo 12 apartado 3)*. A "Guía para as auditorías dos Rexistros Contables de Facturas" da IGAE, establece como un dos obxectivos de ditas auditorías a "Revisión da xestión da seguridade en aspectos relacionados coa confidencialidade, autenticidade, integridade, trazabilidade e dispoñibilidade dos datos e servizos de xestión."

5. Alcance do traballo de revisión

Dada a natureza do obxecto material a revisar, os sistemas de información dun ente público, e a súa gran amplitude e diversidade hoxe día, é necesario concretar que sistemas van revisarse. Por tanto**, na planificación de cada traballo de revisión dos controis básicos de ciberseguridade definirase o alcance concreto** do mesmo de acordo cos obxectivos fixados.

Á hora de seleccionar os sistemas para revisar poderán adoptarse distintos enfoques, dependendo, fundamentalmente, de se a revisión de ciberseguridade está enmarcada no ámbito dunha auditoría financeira, dun proceso en concreto ou dunha auditoría operativa ou, pola contra, trátase dunha auditoría horizontal de ciberseguridade.

Atendendo ao anterior, os criterios xerais para definir o alcance serán os seguintes:

a) No contexto dunha auditoría financeira, seleccionaranse:

- Os sistemas que sustentan os procesos de xestión máis relevantes desde o punto de vista das necesidades do control externo das contas públicas (por exemplo: contabilidade, persoal-nóminas, compras, xestión de ingresos).
- Unha mostra de sistemas que, sen dar soporte específico aos procesos de xestión, son elementos críticos da contorna de TI de calquera ente.

A revisión dos 8 CBCS debería incluírse como **procedemento mínimo obrigatorio** en todas as fiscalizacións de regularidade dos OCEX, xa que os riscos de ciberseguridade deben ter unha especial consideración en todas as auditorías financeiras.

b) No marco dunha auditoría dun proceso específico ou unha auditoría operativa:

- Os sistemas directamente relacionados coa actividade da entidade, (por exemplo, nun hospital as aplicacións de xestión de historias médicas, de asistencia médica, etc.; nun concello a xestión tributaria, o padrón, etc. nunha universidade as matrículas, os expedientes académicos, etc.)
- Unha mostra de sistemas que, sen dar soporte específico aos procesos de xestión, son elementos críticos da contorna de TI de calquera ente.

c) No caso dunha auditoría horizontal sobre ciberseguridade seleccionaranse:

- Os sistemas que se espere que teñan todos os entes a revisar, con obxecto de poder realizar análises comparativas.
- Unha mostra de sistemas que, sen dar soporte específico aos procesos de xestión, son elementos críticos da contorna de TI de calquera ente.

Para os distintos procesos de xestión seleccionados, a revisión debe incluír necesariamente os controis relacionados con:

- a aplicación informática de xestión
- a base de datos subxacente
- os sistemas operativos instalados en cada un dos sistemas que integren a aplicación de xestión (ex. servidor web, servidor de aplicación, servidor de base de datos)

E para a mostra dos sistemas de información non específicos dun determinado proceso de xestión, senón que forman parte da infraestrutura TI xeral, que dá servizo a todos os procesos de xestión dunha entidade, considerararanse os seguintes tipos de elementos:

- controlador de dominio
- software de virtualización
- equipos de usuario
- elementos da rede de comunicacións (ex. router, switches, punto de acceso a rede wifi, etc.)
- elementos de seguridade (ej: firewall, IPS, proxy de correo, proxy de navegación, servidores de autenticación, infraestrutura de xeración de certificados, etc.)

Lembremos que a estrutura simplificada dun sistema de información pode representarse así:

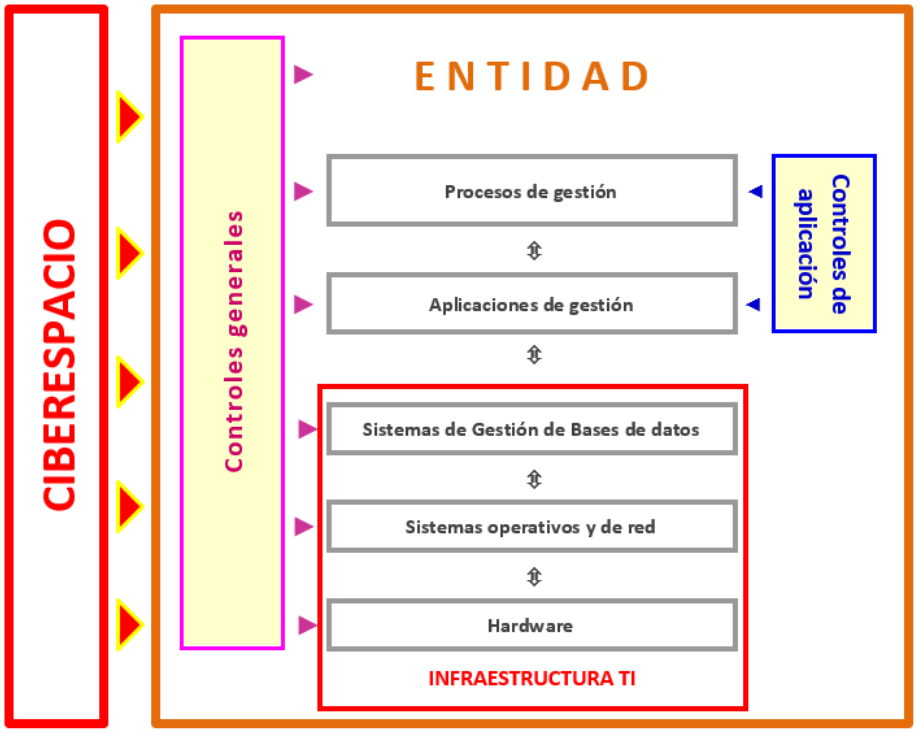

Figura 3

Por último, sinalar que os sistemas seleccionados sempre deberán estar incluídos no ámbito de aplicación do ENS[11], e estar clasificados nas categorías media e alta segundo o ENS.

A modo de resumo, destacar que, en función do tipo de auditoría e o nivel de profundidade da revisión, definirase o alcance concreto do traballo, que **deberá quedar claramente documentado tanto nos papeis de traballo e reflectido no informe resultado do mesmo**.

6. Procedementos de auditoría e programa de traballo

Deberase manter unha reunión cos responsables da entidade para explicar o traballo que se vai a realizar, na cal se entregará o cuestionario do Anexo 4 para que sexa cuberto polo responsable de seguridade da entidade auditada, quen deberá estar presente na reunión.

Posteriormente, tras analizar o cuestionario, cubrirase o **programa de traballo do Anexo 3**, para o que en xeral, os auditores deberán manter outras reunións cos distintos responsables e obteranse as evidencias precisas.

Estes procedementos deberán ser levados a cabo por persoal especializado, idóneamente por auditores de sistemas de información ou por informáticos que presten apoio aos auditores. De non dispoñer de persoal especializado nos OCEX, deberase contar con especialistas externos.

Determinadas comprobacións poderán darse por cumpridas se a entidade presenta as legalmente obrigatorias auditorías de seguridade (ENS).

Confianza nas auditorías do ENS.

Dado que os CBCS están aliñados co ENS, cando a súa revisión se realice en entidades que pasasen a auditoría de seguridade obrigatoria establecida no artigo 34 do RD 3/2010 polo que se aproba o ENS, a revisión poderá basearse, na medida do posible, nos resultados de dita auditoría.

[11] Véxase a guía GCN-STIC-830

Para os efectos da presente guía, para depositar confianza en ditas auditorías deberán cumprir cos requisitos legalmente establecidos[12], entre outros, as entidades certificadoras deberán estar acreditadas e constar na sección Entidades de certificación acreditadas da páxina web do CCN.

Se depositamos confianza nestas auditorías deberá sinalarse expresamente no informe.

7. Avaliación dos achados de auditoría

Os resultados do traballo analizaranse e avaliaranse a dous niveis:

a) Cada un dos CBCS sinalados nas Figuras 1 e 2 está composto por unha serie de subcontrois ou controis detallados, que están relacionados nas fichas de revisión do Anexo 3. Nestas fichas débese documentar o traballo realizado e concluír para cada subcontrol, en base ás evidencias obtidas sobre a súa eficacia, podendo atoparse cada un deles nalgunha das seguintes situacións:

- Control efectivo
- Control bastante efectivo
- Control pouco efectivo
- Control non efectivo ou non implantado

b) Os CBCS son controis globais (compostos por subcontrois) e avaliarase cada un deles utilizando o modelo de nivel de madurez (ver Anexo 4). Para avaliar o seu 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 do CBCS.

Seguiranse os criterios de avaliación establecidos no apartado *8. Avaliación das deficiencias de control interno detectadas*, da GPF-OCEX 5330.

En todo caso, os resultados da revisión dos controis básicos de ciberseguridade comunicaranse de forma detallada ao responsable de seguridade da Entidade.

Se os resultados obtidos de acordo co modelo de nivel de madurez non alcanzan o nivel mínimo de esixencia requirido[13], valorarase a realización dunha auditoría de ciberseguridade de maior amplitude.

[12] Véxanse a Resolución do 27 de marzo de 2018, da Secretaría de Estado de Función Pública, pola que se aproba a Instrución Técnica de Seguridade de Auditoría da Seguridade dos Sistemas de Información, e a Resolución do 13 de outubro de 2016, da Secretaría de Estado de Administracións Públicas, pola que se aproba a Instrución Técnica de Seguridade de conformidade co Esquema Nacional de Seguridade.

[13] Segundo o Infor*me nacional do estado de seguridade dos sistemas das tecnoloxías da información e a comunicación, de 2018*, apartado 3.1, nos diferentes perfís avalíanse os controis mediante un nivel de esixencia, tamén coñecido como nivel de madurez, na aplicación das diferentes medidas de seguridade, e o nivel mínimo de esixencia requirido será:

CATEGORÍA DEL SISTEMA	NIVEL MÍNIMO DE EXIGENCIA REQUERIDO
BÁSICA	L2 – Reproducible, pero intuitivo (50%)
MEDIA	L3 – Proceso definido (80%)
ALTA	L4 – Gestionado y medible (90%)

8. Bibliografía

- Centro Criptolóxico Nacional:
  - Guía CCN-STIC-802, Guía de auditoría do ENS, 2017.
  - Guía CCN-STIC 804, Guía de Implantación do ENS, 2017.
  - Guía CCN-STIC-808, Verificación do cumprimento das medidas no ENS, 2017.
  - Informe nacional do estado de seguridade dos sistemas das tecnoloxías da información e a comunicación, 2018.
- Ciberseguridade. Unha guía de supervisión, Instituto de Auditores Internos de España, 2016.
- Código de Dereito da Ciberseguridade, BOE, xullo 2018.
- Cybersecurity Risk Considerations in a Financial Statement Audit, Institute of Singapore Chartered Accountants, xuño 2018.
- Esquema Nacional de Seguridade .
- GPF-OCEX 5311 Ciberseguridade, seguridade da información e auditoría externa, 27/11/2017.
- ISACA:
  - CIS Controls Audit/Assurance Program, 2017.
  - IS Audit/Assurance Program. Cybersecurity: Based on the NIST Cybersecurity Framework, 2016.
- The Center for Internet Security:
  - The Critical Security Controls for Effective Cyber Defense, Version 7, 19/3/2018.
  - CIS Controls Measures and Metrics for Version 7, 2018.
  - Guide to the First 5 CIS Controls (v6.1), 2017.
- Real Decreto-lei 12/2018, do 7 de setembro, de seguridade das redes e sistemas de información.
- SANS Institute, Back to Basics: Focus on the First Six CIS Critical Security Controls, xaneiro 2017.

Anexo 1. Por que son importantes os controis básicos de ciberseguridade (CBCS)[14]

CBCS 1 Inventario e control de dispositivos físicos

Obxectivo de control: Xestionar activamente (inventariar, revisar e corrixir) todos os dispositivos hardware na rede, de forma que só os dispositivos autorizados teñan acceso á rede.

Este control axuda ás organizacións para definir a base do que hai que defender. Sen coñecer que dispositivos están conectados, non poden ser defendidos.

O inventario debe ser tan completo como sexa posible: en organizacións cun nivel de madurez básico o inventario pode ser realizado e mantido con procedementos manuais e, noutras máis maduras, utilizando ferramentas de escaneo (tanto activos como pasivos) que detecten os dispositivos conectados á rede corporativa.

En calquera caso, o obxectivo inicial do control é coñecer o que está na rede para que poida ser defendido e, posteriormente, impedir que dispositivos non autorizados se unan á rede.

Por que é importante este control?

Os atacantes, que poden estar situados en calquera parte do mundo, están escaneando continuamente as redes das organizacións obxectivo, esperando que novos e desprotexidos sistemas se incorporen a esas redes. Buscan dispositivos, como os portátiles, que se conectan e desconectan das redes corporativas, e é máis probable que non dispoñan dos últimos parches e actualizacións de seguridade, aproveitando o lapso trascurrido ata a súa actualización.

Outros dispositivos que se conectan á rede corporativa (p.e. sistemas para demostracións, redes para convidados, etc.) deben ser xestionados con coidado ou illados para previr accesos non autorizados que comprometan a seguridade.

Os dispositivos persoais dos empregados (portátiles, tabletas, móbiles) que se conecten á rede corporativa tamén poden verse comprometidos e ser usados para infectar os recursos internos.

O adecuado control de todos os dispositivos tamén xoga un papel crítico na planificación e execución das copias de seguridade do sistema e na súa recuperación.

Que di o ENS?

"Artigo 20. Integridade e actualización do sistema

1. Todo elemento físico ou lóxico requirirá autorización formal previa á súa instalación no sistema."

Medidas de seguridade:

"4.3.1 Inventario de activos (op.exp.1)

Manterase un inventario actualizado de todos os elementos do sistema, detallando a súa natureza e identificando o seu responsable; é dicir, a persoa que é responsable das decisións relativas ao mesmo."

Guía CCN-STIC 804: 4.3.1 [OP.EXP.1] INVENTARIO DE ACTIVOS

"183. O inventario debe cubrir todo o dominio de seguridade do responsable da seguridade do sistema de información, ata alcanzar os puntos de interconexión e os servizos prestados por terceiros. A granularidade debe ser suficiente para cubrir as necesidades de reporte de incidentes e para facer un seguimento, tanto formal (auditorías) como reactivo no proceso de xestión de incidentes.

- Identificación do activo: fabricante, modelo, número de serie
- Configuración do activo: perfil, política, software instalado
- Software instalado: fabricante, produto, versión e parches aplicados
- Equipamento de rede: MAC, IP asignada (ou rango)

[14] Fonte: *The Critical Security Controls for Effective Cyber Defense, Esquema Nacional de Seguridade* e elaboración propia.

- Localización do activo: onde está?
- Propiedade do activo: persoa responsable do mesmo."

CBCS 2 **Inventario e control de software autorizado e non autorizado**

Obxectivo de control: Xestionar activamente (inventariar, revisar e corrixir) todo o software na rede, de forma que só se poida instalar e executar software autorizado e que o non autorizado sexa detectado e se evite a súa instalación e execución.

A finalidade deste control é asegurar que só está permitido executar software autorizado nos sistemas da organización impedindo a execución de software potencialmente vulnerable.

Manter un inventario de software é importante, e dispoñer dunha lista branca de aplicacións autorizadas é un factor crucial deste proceso, xa que limita a capacidade de executar aplicacións unicamente a aquelas que están expresamente autorizadas.

Aínda que non é unha solución máxica para a defensa, este control a miúdo considérase un dos máis eficaces para a prevención e detección de ciberataques.

A implementación do control a miúdo require que as organizacións reconsideren as súas políticas e a súa cultura, os usuarios xa non poderán instalar o software que desexen. Pero este control está implementado con éxito por numerosas organizacións, e probablemente axudará a previr e detectar ciberataques.

Por que é importante este control?

Os atacantes escanean continuamente as organizacións obxectivo buscando versións vulnerables de software que poidan explotarse remotamente. Algúns atacantes tamén distribúen páxinas web hostís, arquivos de documentos, arquivos multimedia e outros contidos a través das súas propias páxinas web ou sitios de terceiros de confianza. Cando as vítimas desprevidas acceden a este contido cun navegador vulnerable ou outro programa, os atacantes comprometen as súas máquinas, a miúdo instalando programas ocultos e bots[15] que lle dan ao atacante un control a longo prazo do sistema. Sen o coñecemento ou o control apropiados do software despregado nunha organización, os defensores non poden asegurar adecuadamente os seus activos.

É máis probable que as máquinas mal controladas estean a executar software que non sexa necesario para os fins da entidade (introducindo posibles fallos de seguridade), ou executando malware introducido por un atacante despois de que un sistema foi comprometido.

Unha vez que unha máquina foi comprometida, os atacantes utilízana a miúdo como punto para recoller información sensible do sistema no que está integrada e doutros sistemas conectados a el. Ademais, as máquinas comprometidas utilízanse como punto de lanzamento para o movemento a través da rede e das redes conectadas. Desta maneira, os atacantes poden rapidamente converter unha máquina comprometida en moitas.

As organizacións que non teñen inventarios completos de software non poden atopar software vulnerable ou malicioso para mitigar problemas ou eliminar aos atacantes.

O control de todo o software tamén desempeña un papel fundamental na planificación e execución de copias de seguridade e na recuperación do sistema.

As listas brancas protexen os sistemas de información de que aplicacións non autorizadas se executen neles, protexéndoos de aplicacións daniñas. Son aplicables a servidores, equipos de sobremesa e portátiles.

Que di o ENS?

"Artigo 20. Integridade e actualización do sistema

1. Todo elemento físico ou lóxico requirirá autorización formal previa á súa instalación no sistema.

[15] Segundo Wikipedia un bot (aférese de robot) é un programa informático que efectúa automaticamente tarefas repetitivas a través de Internet.

2. Deberase coñecer en todo momento o estado de seguridade dos sistemas, en relación ás especificacións dos fabricantes, ás vulnerabilidades e ás actualizacións que lles afecten, reaccionando con dilixencia para xestionar o risco á vista do estado de seguridade dos mesmos."

Medidas de seguridade:

"4.3.1 Inventario de activos (op.exp.1)

Manterase un inventario actualizado de todos os elementos do sistema, detallando a súa natureza e identificando o seu responsable; é dicir, a persoa que é responsable das decisións relativas ao mesmo."

Guía CCN-STIC 804: 4.3.1 [OP.EXP.1] INVENTARIO DE ACTIVOS

"183. O inventario debe cubrir todo o dominio de seguridade do responsable da seguridade do sistema de información, ata alcanzar os puntos de interconexión e os servizos prestados por terceiros. A granularidade debe ser suficiente para cubrir as necesidades de reporte de incidentes e para facer un seguimento, tanto formal (auditorías) como reactivo no proceso de xestión de incidentes.

- Identificación do activo: fabricante, modelo, número de serie
- Configuración do activo: perfil, política, software instalado
- **Software instalado: fabricante, produto, versión e parches aplicados**
- Equipamento de rede: MAC, IP asignada (ou rango)
- Localización do activo: onde está?
- Propiedade do activo: persoa responsable do mesmo."

CBCS 3 Proceso continuo de identificación e remediación de vulnerabilidades

Obxectivo de control: Dispoñer dun proceso continuo para obter información sobre novas vulnerabilidades, identificalas, remedialas e reducir a xanela de oportunidade aos atacantes.

O obxectivo deste control é coñecer e eliminar debilidades técnicas que existen nos sistemas de información da organización, reducindo a probabilidade de que os sistemas sigan sendo vulnerables.

As organizacións punteiras implementan sistemas de administración de parches e actualizacións que cobren vulnerabilidades tanto de sistemas operativos como aplicacións de terceiros.

Isto permite de forma automática, continua e proactiva a instalación de actualizacións para solucionar vulnerabilidades do software.

As organizacións deben implementar ferramentas de xestión de vulnerabilidades para dotarse da capacidade de detectar e remediar debilidades de software explotables.

Por que é importante este control?

Os ciberdefensores deben operar nun fluxo constante de información nova: actualizacións de software, parches, avisos de seguridade, boletíns de ameazas, etc. A comprensión e xestión das vulnerabilidades converteuse nunha actividade continua, que require tempo, atención e recursos significativos.

Os atacantes teñen acceso á mesma información e poden aproveitar as brechas entre a aparición de novos coñecementos e a remediación. Por exemplo, cando os investigadores reportan novas vulnerabilidades, comeza unha carreira entre todas as partes, incluíndo: atacantes (para "armarse", despregar un ataque, e explotalo); provedores (para desenvolver, implementar parches ou firmas e actualizacións), e defensores (para avaliar riscos, parches de proba, e instalalos).

As organizacións que non escanean as vulnerabilidades e abordan de forma proactiva os defectos atopados enfróntanse a unha alta probabilidade de que os seus sistemas informáticos sexan comprometidos. Os defensores enfróntanse a desafíos particulares en canto a escalar o remedio en toda unha entidade, e priorizar as accións con conflitos de prioridades e, ás veces, efectos secundarios incertos.

Qué di o ENS?

"Artigo 20. Integridade e actualización do sistema

2. Deberase coñecer en todo momento o estado de seguridade dos sistemas, en relación ás especificacións dos fabricantes, ás vulnerabilidades e ás actualizacións que lles afecten, reaccionando con dilixencia para xestionar o risco á vista do estado de seguridade dos mesmos."

Medidas de seguridade:

"5.6.2 Aceptación e posta en servizo (mp.sw.2)

Categoría BÁSICA

Antes de pasar a produción comprobarase o correcto funcionamento da aplicación.

a) Comprobarase que:

1.º Cúmprense os criterios de aceptación en materia de seguridade.

2.º Non se deteriora a seguridade doutros compoñentes do servizo.

b) As probas realizaranse nunha contorna illada (preprodución).

c) As probas de aceptación non se realizarán con datos reais, salvo que se asegure o nivel de seguridade correspondente.

Categoría MEDIA

Realizaranse as seguintes inspeccións previas á entrada en servizo:

a) Análise de vulnerabilidades.

b) Probas de penetración.

Categoría ALTA

Realizaranse as seguintes inspeccións previas á entrada en servizo:

a) Análise de coherencia na integración nos procesos.

b) Considerarase a oportunidade de realizar unha auditoría de código fonte."

"4.3.3 Xestión da configuración (op.exp.3)

Xestionarase de forma continúa a configuración dos compoñentes do sistema de forma que:

d) O sistema reaccione a vulnerabilidades reportadas ([op.exp.4])."

"4.3.4 Mantemento (op.exp.4)

Para manter o equipamento físico e lóxico que constitúe o sistema, aplicarase o seguinte:

a) Atenderase ás especificacións dos fabricantes no relativo a instalación e mantemento dos sistemas.

b) Efectuarase un seguimento continuo dos anuncios por defectos.

c) Dispoñerase dun procedemento para analizar, priorizar e determinar cando aplicar as actualizacións de seguridade, parches, melloras e novas versións. A priorización terá en conta a variación do risco en función da aplicación ou non da actualización."

Guía CCN-STIC 804: "4.3.4 [OP.EXP.4] MANTEMENTO

199. Proactivamente deberase estar informado dos defectos anunciados por parte do fabricante ou provedor (por exemplo mediante subscricións a listas de correo ou RSS, consultando noticias en webs de tecnoloxía, seguridade ou fabricantes, etc.).

200. Deberá existir un procedemento para establecer cando implantar os cambios e determinar a súa prioridade e urxencia proporcionada ao risco que implica a súa non aplicación (cambios preaprobados, cambios de emerxencia, etc.)."

CBCS 4 **Uso controlado de privilexios administrativos**

Obxectivo de control: Desenvolver procesos e utilizar ferramentas para identificar, controlar, previr e corrixir o uso, asignación e configuración de privilexios administrativos en computadores, redes e aplicacións.

Este control garante que os privilexios de administración de sistemas estean asignados unicamente aos empregados que os necesitan, en base ás funcións que desempeñan, e que a entidade poida atribuír as accións administrativas a usuarios individuais.

Desafortunadamente, para facilitar a axilidade e a comodidade, moitas organizacións permiten que o seu persoal teña dereitos de administrador tanto a nivel da aplicación de xestión, como nos sistemas que lle dan soporte (sistema operativo, base de datos, etc.) así como nos seus equipos.

A situación anterior deriva na existencia do risco de acceso e cambios non autorizados aos sistemas, que pode materializarse desde dous puntos diferentes:

- Desde o punto de vista externo, cuxa porta de entrada é o usuario, e no que se aproveitan os privilexios de administración dos usuarios nos seus equipos, para acceder desde fóra á rede interna da entidade.
- Desde o punto de vista interno, é dicir, desde dentro da rede da entidade (ben por parte dun empregado con acceso autorizado ou ben como consecuencia dun ciberataque que se iniciou externamente aproveitando a debilidade descrita no parágrafo anterior). Neste caso, a xestión inadecuada dos privilexios de administración nos sistemas operativos, base de datos, etc. dá aos atacantes a oportunidade de acceder e realizar cambios non autorizados nos sistemas corporativos que sustentan os procesos de xestión.

Este control lévanos a que as contas de usuarios administradores de aplicacións, bases de datos, sistemas operativos e equipos de usuario 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.

Por que é importante este control?

O uso inadecuado de privilexios administrativos é un método primario para que os atacantes se propaguen dentro dunha entidade obxectivo. Dúas técnicas de ataque moi comúns aproveitan os privilexios administrativos incontrolados.

Na primeira, un usuario que opera como administrador do seu equipo, abre un adxunto de correo electrónico malicioso, descarga e abre un arquivo dun sitio web malicioso, ou simplemente navega nun sitio web que aloxa contido do atacante que pode explotar automaticamente navegadores. O arquivo ou exploit contén código executable que se executa no equipo da vítima xa sexa automaticamente ou enganando ao usuario para que execute o contido do atacante. Se a conta do usuario da vítima ten privilexios administrativos, o atacante pode apoderarse completamente da máquina da vítima e instalar os rexistradores de teclas, os sniffers e o software de control remoto para atopar contrasinais administrativos e outros datos sensibles. Ataques similares ocorren co correo electrónico. Un administrador abre inadvertidamente un correo electrónico que contén un arquivo adxunto infectado e utilízase para obter un punto de pivote dentro da rede que se utiliza para atacar outros sistemas.

A segunda técnica común utilizada polos atacantes é a elevación de privilexios ao adiviñar ou romper un contrasinal dun usuario administrativo para conseguir o acceso a un equipo de destino. Se os privilexios administrativos distribúense de forma folgada e ampla, ou son idénticos aos contrasinais utilizados en sistemas menos críticos, ao atacante cústalle moito menos tomar o control total dos sistemas, porque hai moitas máis contas que poden actuar como vías para o atacante para comprometer privilexios administrativos.

A revisión deste control pode orientarse a verificar a existencia dunha política de alta, baixa e mantemento de usuarios administradores, e a fortaleza dos contrasinais e as tarefas que se desenvolven para comprobar o seu cumprimento.

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.

Que di o ENS?

"Artigo 16. Autorización e control dos accesos.

O acceso ao sistema de información deberá ser controlado e limitado aos usuarios, procesos, dispositivos e outros sistemas de información, debidamente autorizados, restrinxindo o acceso ás funcións permitidas."

Medidas de seguridade:

"4.2 Control de acceso (op.acc)

O control de acceso cobre o conxunto de actividades preparatorias e executivas para que unha determinada entidade, usuario ou proceso, poida, ou non, acceder a un recurso do sistema para realizar unha determinada acción.

O control de acceso que se implante nun sistema real será un punto de equilibrio entre a comodidade de uso e a protección da información. En sistemas de nivel Baixo, primarase a comodidade, mentres que en sistemas de nivel Alto primarase a protección.

En todo control de acceso requirirase o seguinte:

a) Que todo acceso estea prohibido, salvo concesión expresa.

b) Que a entidade quede identificada singularmente [op.acc.1].

c) Que a utilización dos recursos estea protexida [op.acc.2].

d) Que se definan para cada entidade os seguintes parámetros: a que se necesita acceder, con que dereitos e baixo que autorización [op.acc.4].

e) Serán diferentes as persoas que autorizan, usan e controlan o uso [op.acc.3].

f) Que a identidade da entidade quede suficientemente autenticada [op.acc.5].

g) Que se controle tanto o acceso local ([op.acc.6]) como o acceso remoto ([op.acc.7]).

Co cumprimento de todas as medidas indicadas garantirase que ninguén accederá a recursos sen autorización. Ademais, quedará rexistrado o uso do sistema ([op.exp.8]) para poder detectar e reaccionar a calquera fallo accidental ou deliberado.

Cando se interconecten sistemas nos que a identificación, autenticación e autorización teñan lugar en diferentes dominios de seguridade, baixo distintas responsabilidades, nos casos en que sexa necesario, as medidas de seguridade locais acompañaranse dos correspondentes acordos de colaboración que delimiten mecanismos e procedementos para a atribución e exercicio efectivos das responsabilidades de cada sistema ([op.ext])."

"4.2.4 Proceso de xestión de dereitos de acceso [op.acc.4].

Os dereitos de acceso de cada usuario, limitaranse atendendo aos seguintes principios:

a) Mínimo privilexio. Os privilexios de cada usuario reduciranse ao mínimo estritamente necesario para cumprir as súas obrigas. Desta forma acoútanse os danos que puidese causar unha entidade, de forma accidental ou intencionada.

b) Necesidade de coñecer. Os privilexios limitaranse de forma que os usuarios só accederán ao coñecemento daquela información requirida para cumprir as súas obrigas.

c) Capacidade de autorizar. Só e exclusivamente o persoal con competencia para iso, poderá conceder, alterar ou anular a autorización de acceso aos recursos, conforme aos criterios establecidos polo seu responsable."

Guía CCN-STIC 804: "4.2.4 [OP.ACC.4] PROCESO DE XESTIÓN DE DEREITOS DE ACCESO

121. Na estruturación dos dereitos de acceso débense en conta as necesidades de cada usuario segundo a súa función na organización e as tarefas que ten encomendadas.

122. A necesidade de acceso debe vir por escrito de parte do responsable da información ou proceso ao que vai concedérselle acceso.

123. O recoñecemento da necesidade de acceso debe ser reasegurado periodicamente, extinguíndose cando non se demostre positivamente que a necesidade perdura.

124. Deberá prestarse unha especial atención ás contas de administración do sistema (administración de equipos, de aplicacións, de comunicacións, de seguridade), establecendo procedementos áxiles de cancelación e mecanismos de monitorización do uso que se fai delas."

"4.2.5 Mecanismo de autenticación [op.acc.5].

Os mecanismos de autenticación fronte ao sistema adecuaranse ao nivel do sistema atendendo ás consideracións que seguen, podendo usarse os seguintes factores de autenticación:

– "algo que se sabe": contrasinais ou claves concertadas.
– "algo que se ten": compoñentes lóxicos (tales como certificados software) ou dispositivos físicos (en expresión inglesa, tokens).
– "algo que se é": elementos biométricos.

Os factores anteriores poderán utilizarse de maneira illada ou combinarse para xerar mecanismos de autenticación forte.

As guías CCN-STIC desenvolverán os mecanismos concretos adecuados para cada nivel.

As instancias do factor ou os factores de autenticación que se utilicen no sistema denominaranse **credenciais**.

Antes de proporcionar as credenciais de autenticación aos usuarios, estes deberán identificarse e rexistrarse de maneira fidedigna ante o sistema ou ante un provedor de identidade electrónica recoñecido pola Administración. Contémplanse varias posibilidades de rexistro dos usuarios:

– Mediante a presentación física do usuario e verificación da súa identidade acorde á legalidade vixente, ante un funcionario habilitado para iso.
– De forma telemática, mediante DNI electrónico ou un certificado electrónico cualificado.
– De forma telemática, utilizando outros sistemas admitidos legalmente para a identificación dos cidadáns dos contemplados na normativa de aplicación.

Nivel BAIXO

a) Como principio xeral, admitirase o uso de calquera mecanismo de autenticación sustentado nun só factor.

b) No caso de utilizarse como factor "algo que se sabe", aplicaranse regras básicas de calidade da mesma.

c) Atenderase á seguridade das credenciais de forma que:

1. As credenciais activaranse unha vez estean baixo o control efectivo do usuario.
2. As credenciais estarán baixo o control exclusivo do usuario.
3. O usuario recoñecerá que as recibiu e que coñece e acepta as obrigas que implica a súa tenencia, en particular, o deber de custodia dilixente, protección da súa confidencialidade e información inmediata en caso de perda.
4. As credenciais cambiaranse cunha periodicidade marcada pola política da organización, atendendo á categoría do sistema ao que se accede.
5. As credenciais retiraranse e serán deshabilitadas cando a entidade (persoa, equipo ou proceso) que autentican termina a súa relación co sistema.

Nivel MEDIO

a) Esixirase o uso de polo menos dous factores de autenticación.

b) No caso de utilización de "algo que se sabe" como factor de autenticación, estableceranse esixencias rigorosas de calidade e renovación.

c) As credenciais utilizadas deberán ser obtidas tras un rexistro previo:

1. Presencial.
2. Telemático usando certificado electrónico cualificado.
3. Telemático mediante unha autenticación cunha credencial electrónica obtida tras un rexistro previo presencial ou telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO

a) As credenciais suspenderanse tras un período definido de non utilización.

b) No caso do uso de utilización de "algo que se ten", requirirase o uso de elementos criptográficos hardware usando algoritmos e parámetros acreditados polo Centro Criptolóxico Nacional.

c) As credenciais utilizadas deberán ser obtidas tras un rexistro previo presencial ou telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma."

"4.3.8 Rexistro da actividade dos usuarios (op.exp.8) #SÓ ADMINISTRADORES DE SISTEMAS#

Rexistraranse as actividades dos usuarios no sistema, de forma que:

a) O rexistro indicará quen realiza a actividade, cando a realiza e sobre que información.

b) Incluirase a actividade dos usuarios e, especialmente, a dos operadores e administradores en canto poidan acceder á configuración e actuar no mantemento do sistema.

c) Deberán rexistrarse as actividades realizadas con éxito e os intentos fracasados.

d) A determinación de que actividades deben rexistrarse e con que niveis de detalle adoptarase á vista da análise de riscos realizado sobre o sistema ([op.pl.1]).

Nivel MEDIO (dimensión trazabilidade)

Revisaranse informalmente os rexistros de actividade buscando patróns anormais.

Nivel ALTO (dimensión trazabilidade)

Dispoñerase dun sistema automático de recolección de rexistros e correlación de eventos; é dicir, unha consola de seguridade centralizada."

CBCS 5 Configuracións seguras do hardware e software de dispositivos móbiles, portátiles, equipos de sobremesa e servidores

Obxectivo de control: 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.

Por defecto, a maioría dos sistemas están configurados para facilitar o seu uso e non necesariamente pensando na seguridade. Para implantar este control, as organizacións necesitan reconfigurar os sistemas de acordo con estándares de seguridade.

Por que é importante este control?

Tal como o entregan os fabricantes e vendedores, as configuracións predeterminadas para os sistemas operativos e as aplicacións están normalmente orientadas á facilidade de implementación e á facilidade de uso, non á seguridade. Cando se entrega un software é habitual atoparse con controis pouco robustos, servizos e portos abertos, contas ou contrasinais predeterminadas, protocolos antigos (vulnerables), preinstalación de software innecesario; todos estes aspectos son vulnerables no seu estado predeterminado.

O desenvolvemento de opcións de configuración con boas propiedades de seguridade é unha tarefa complexa máis aló da capacidade dos usuarios individuais, requirindo análises ás veces complexas para tomar boas decisións.

Mesmo se se desenvolve e instala unha configuración inicial forte, debe ser revisada e actualizada continuamente para evitar a deterioración da seguridade, en particular cando o software é actualizado ou parcheado, divúlganse as novas vulnerabilidades da seguridade, ou as configuracións se "axustan" para permitir a instalación de novo software ou para dar soporte a novos requirimentos operacionales. Se non se revisa e actualiza de forma continua, os atacantes atoparán oportunidades para explotar tanto os servizos accesibles á rede como o software cliente.

Que di o ENS?

"Artigo 19. Seguridade por defecto.

Os sistemas deben deseñarse e configurarse de forma que garantan a seguridade por defecto:

a) O sistema proporcionará a mínima funcionalidade requirida para que a organización alcance os seus obxectivos.

b) As funcións de operación, administración e rexistro de actividade serán as mínimas necesarias, e asegurarase que só son accesibles polas persoas, ou desde emprazamentos ou equipos, autorizados, podendo esixirse no seu caso restricións de horario e puntos de acceso facultados.

c) Nun sistema de explotación eliminaranse ou desactivaranse, mediante o control da configuración, as funcións que non sexan de interese, sexan innecesarias e, mesmo, aquelas que sexan inadecuadas ao fin que se persegue.

d) O uso ordinario do sistema será sinxelo e seguro, de forma que unha utilización insegura requira dun acto consciente por parte do usuario."

Medidas de seguridade:

"4.3.2 Configuración de seguridade (op.exp.2)

Configuraranse os equipos previamente á súa entrada en operación, de forma que:

a) Retírense contas e contrasinais estándar.

b) Aplicarase a regra de «mínima funcionalidade»:

1.º O sistema debe proporcionar a funcionalidade requirida para que a organización alcance os seus obxectivos e ningunha outra funcionalidade,

2.º Non proporcionará funcións gratuítas, nin de operación, nin de administración, nin de auditoría, reducindo desta forma o seu perímetro ao mínimo imprescindible.

3.º Eliminarase ou desactivarase mediante o control da configuración aquelas funcións que non sexan de interese, non sexan necesarias, e mesmo, aquelas que sexan inadecuadas ao fin que se persegue.

c) Aplicarase a regra de «seguridade por defecto»:

1.º As medidas de seguridade serán respectuosas co usuario e protexerán a este, salvo que se expoña conscientemente a un risco.

2.º Para reducir a seguridade, o usuario ten que realizar accións conscientes.

3.º O uso natural, nos casos que o usuario non consultou o manual, será un uso seguro."

Guía CCN-STIC 804: "4.3.2 [OP.EXP.2] CONFIGURACIÓN DE SEGURIDADE

187. Todos os sistemas deben ser configurados de forma sistemática antes de entrar en produción. O organismo debe elaborar uns poucos perfís de configuración para as diferentes actividades a que poden ser dedicados, sendo típicos os seguintes:

- usuarios normais (uso administrativo)
- atención a clientes
- xestión de provedores (incluídos bancos)
- desenvolvemento
- operadores e administradores (técnicos de sistemas)
- responsable de seguridade (consola de configuración)
- auditoría

188. A medida instruméntase por medio dunha lista de verificación (checklists) que se debe aplicar sistematicamente a cada equipo antes de entrar en produción.

189. En todos os perfís de usuario, excepto nos de administrador, débese bloquear a opción de que este poida cambiar a configuración do sistema ou poida instalar novos programas ou novos periféricos (drivers).

190. A configuración de seguridade debe incluír un perfil básico de auditoría de uso do equipo."

"4.3.3 Xestión da configuración (op.exp.3)

(Categoría Media)

Xestionarase de forma continúa a configuración dos compoñentes do sistema de forma que:

a) Mantéñase en todo momento a regra de "funcionalidade mínima" ([op.exp.2]).
b) Mantéñase en todo momento a regra de "seguridade por defecto" ([op.exp.2]).
c) O sistema se adapte ás novas necesidades, previamente autorizadas ([op.acc.4]).
d) O sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).
e) O sistema reaccione a incidentes (ver [op.exp.7])."

CBCS 6 Rexistro da actividade dos usuarios (Mantemento, monitorización e análise dos LOG de auditoría)

Obxectivo de control: Recoller, xestionar e analizar logs de eventos que poden axudar a detectar, entender ou recuperarse dun ataque.

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.

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 dispoñer dun SIEM (Security Information and Event Management), sistema que permite dispoñer en tempo real de alertas de seguridade.

A maioría dos sistemas operativos, servizos de rede e firewall, tanto libres como comerciais, ofrecen capacidades de log, pero tales rexistros deben ser activados. Firewalls, proxies e sistemas de acceso remoto (VPN, telefónico, etc.) deben ser configurados para o rexistro detallado e almacenar toda a información dispoñible para o caso dunha investigación. Ademais, os sistemas operativos, especialmente os de servidores, deben estar configurados para crear rexistros de control de acceso cando un usuario tenta acceder a recursos sen os privilexios adecuados. Para avaliar se tal rexistro está operativo, a organización debe escanear periodicamente as súas logs e comparalos co inventario de activos instalado como parte do Control 1 para asegurar que cada elemento conectado á rede está a xerar periodicamente logs.

Os programas analíticos para revisar rexistros poden ser valiosos, pero os medios empregados para analizar os logs de auditoría son bastante diversos, incluso un rápido exame realizado por unha persoa é importante para esa finalidade. As ferramentas de correlación poden facer moito máis útiles os rexistros de auditoría para unha posterior inspección manual. Tales ferramentas poden ser moi útiles na identificación de ataques sutís. Con todo, estas ferramentas non son unha panacea nin unha substitución para os administradores de sistemas e persoal experimentado de seguridade da información. Mesmo con ferramentas de análises de rexistro automatizado, requírese a intuición e experiencia humana para identificar e comprender os ataques.

Por que é importante este control?

Deficiencias no rexistro de seguridade e na súa análise permiten aos atacantes ocultar a súa localización, o software malicioso introducido e as actividades ilícitas que realizan nas máquinas vítimas. Mesmo se as vítimas saben que os seus sistemas foron comprometidos, sen rexistros de logs completos e protexidos, permanecen cegos aos detalles do ataque e ás posteriores accións dos atacantes.

Sen uns logs de auditoría sólidos, un ataque pode pasar desapercibido por tempo indefinido e os danos infrinxidos poden ser irreversibles.

Ás veces estes rexistros son a única evidencia dun ataque exitoso. Moitas organizacións manteñen os rexistros de auditoría para fins de cumprimento, pero os atacantes confían no feito de que estas organizacións de cando en cando analizan os rexistros de auditoría, polo que non saben que os seus sistemas foron comprometidos. Debido a deficientes ou inexistentes procesos de análises de rexistros, os atacantes controlan ás veces máquinas vítima durante meses ou anos sen que ninguén se decate na organización do destino, a pesar de que a evidencia do ataque rexistrouse nos ditos rexistros non examinados.

Que di o ENS?

"Artigo 23. Rexistro de actividade

Coa finalidade exclusiva de lograr o cumprimento do obxecto do presente real decreto, con plenas garantías do dereito á honra, á intimidade persoal e familiar e á propia imaxe dos afectados, e de acordo coa normativa sobre protección de datos persoais, de función pública ou laboral, e demais disposicións que resulten de aplicación, rexistraranse as actividades dos usuarios, retendo a información necesaria para monitorar, analizar, investigar e documentar actividades indebidas ou non autorizadas, permitindo identificar en cada momento á persoa que actúa."

Medidas de seguridade:

"4.3.8 Rexistro da actividade dos usuarios (op.exp.8)

Rexistraranse as actividades dos usuarios no sistema, de forma que:

a) O rexistro indicará quen realiza a actividade, cando a realiza e sobre que información.
b) Incluirase a actividade dos usuarios e, especialmente, a dos operadores e administradores en canto poidan acceder á configuración e actuar no mantemento do sistema.
c) Deberán rexistrarse as actividades realizadas con éxito e os intentos fracasados.
d) A determinación de que actividades deben rexistrarse e con que niveis de detalle se adoptará á vista da análise de riscos realizado sobre o sistema ([op.pl.1]).

Nivel MEDIO (dimensión trazabilidade)

Revisaranse informalmente os rexistros de actividade buscando patróns anormais.

Nivel ALTO (dimensión trazabilidade)

Dispoñerase dun sistema automático de recolección de rexistros e correlación de eventos; é dicir, unha consola de seguridade centralizada."

Guía CCN-STIC 804: "4.3.8 [OP.EXP.8] REXISTRO DA ACTIVIDADE DOS USUARIOS

225. Realízase unha inspección regular dos rexistros para identificar anomalías no uso dos sistemas (uso irregular ou non previsto)

226. Utilízanse ferramentas automáticas para recoller e analizar os rexistros en busca de actividades fóra do normal (por exemplo: consola de seguridade centralizada, SIEM)."

"4.3.10 Protección dos rexistros de actividade [op.exp.10].

Nivel ALTO

Protexeranse os rexistros do sistema, de forma que:

a) Determinarase o período de retención dos rexistros.
b) Asegurarase a data e hora. Ver [mp.info.5].
c) Os rexistros non poderán ser modificados nin eliminados por persoal non autorizado.
d) As copias de seguridade, se existen, axustaranse aos mesmos requisitos."

Guía CCN-STIC 804: "4.3.10 [OP.EXP.10] PROTECCIÓN DOS REXISTROS DE ACTIVIDADE

236. Deberanse reter os rexistros de maneira adecuada:

- existe unha declaración formal dos períodos de retención habituais
- existe un plan para garantir a capacidade de almacenamento de rexistros atendendo ao seu volume e política de retención

- existe un procedemento formal para a retención de evidencias tras un incidente

237. Existen mecanismos que garantan a corrección da hora á que se realiza o rexistro, en prevención de manipulacións dos reloxos.

238. Unicamente o persoal autorizado poderá modificar ou eliminar os rexistros:

- existen mecanismos para previr o acceso aos rexistros de persoas non autorizadas
- existen mecanismos para previr o acceso de persoas non autorizadas á configuración do sistema para o rexistro automático de actividades
- existe un procedemento para a eliminación dos rexistros tras o período estipulado de retención, incluíndo as copias de seguridade

239. Os rexistros están contemplados nos procesos de copias de seguridade, garantindo as seguridades antes mencionadas."

CBCS 7 **Copias de seguridade de datos e sistemas**

Obxectivo de control: Utilizar procesos e ferramentas para realizar a copia de seguridade da información crítica cunha metodoloxía probada que permita a recuperación da información en tempo oportuno.

Por que é importante este control?

Cando os atacantes comprometen os sistemas, a miúdo realizan cambios significativos das configuracións e o software. En ocasións, os atacantes tamén realizan alteracións sutís dos datos almacenados nos sistemas comprometidos, o que pode poñer en perigo a eficacia da organización con información contaminada.

Cando se descobre aos atacantes, pode ser extremadamente difícil para as organizacións sen unha capacidade confiable de recuperación de datos eliminar todos os aspectos da presenza do atacante nos sistemas.

Outras consideracións

Periodicamente, por exemplo, trimestralmente, e cada vez que se compra un novo sistema para a realización de copias de seguridade, un equipo de probas debe avaliar unha mostra aleatoria das copias de seguridade realizadas tentando restauralas nunha contorna probas. As **probas de recuperación** dos sistemas restaurados deben incluír a verificación non só do proceso de recuperación, senón tamén do seu contido, é dicir, que o sistema operativo, a aplicación e os datos da copia de seguridade estean intactos e sexan funcionais.

Os ciberataques mediante ransomware vólvense inefectivos cando se dispón de copia de seguridade dos datos secuestrados. Por iso, os ciberdelincuentes melloraron os programas que utilizan para cifrar, de forma que estes conéctanse a todos os repositorios accesibles vía a rede de comunicacións, co fin de conseguir cifrar tamén os backups. Este tipo de ataques "mellorados" foi utilizado con efectos devastadores nas últimas ondas de ransomware. Por iso, o contar cunha copia de seguridade que non se atope accesible a nivel de rede, é dicir, atópese illada, é unha medida de protección adicional ás de cifrado e seguridade física.

Que di o ENS?

"Artigo 7. Prevención, reacción e recuperación.

4. As medidas de recuperación permitirán a restauración da información e os servizos, de forma que se poida facer fronte ás situacións nas que un incidente de seguridade inhabilite os medios habituais."

"Artigo 21. Protección de información almacenada e en tránsito

2. Forman parte da seguridade os procedementos que aseguren a recuperación e conservación a longo prazo dos documentos electrónicos producidos polas Administracións públicas no ámbito das súas competencias."

"Artigo 25. Continuidade da actividade.

Os sistemas dispoñerán de copias de seguridade e establecerán os mecanismos necesarios para garantir a continuidade das operacións, en caso de perda dos medios habituais de traballo."

Medidas de seguridade:

"5.7.7 Copias de seguridade (mp.info.9)

Realizaranse copias de seguridade que permitan recuperar datos perdidos, accidental ou intencionadamente cunha antigüidade determinada.

Estas copias posuirán o mesmo nivel de seguridade que os datos orixinais no que se refire a integridade, confidencialidade, autenticidade e trazabilidade. En particular, considerarase a conveniencia ou necesidade, segundo proceda, de que as copias de seguridade estean cifradas para garantir a confidencialidade.

As copias de seguridade deberán abarcar:

a) Información de traballo da organización.
b) Aplicacións en explotación, incluíndo os sistemas operativos.
c) Datos de configuración, servizos, aplicacións, equipos, ou outros de natureza análoga.
d) Claves utilizadas para preservar a confidencialidade da información."

Guía CCN-STIC 804: "5.7.7 [MP.INFO.9] COPIAS DE SEGURIDADE (BACKUP)

596. Débense realizar copias de respaldo que permitan recuperar datos perdidos accidental ou intencionadamente cunha antigüidade para determinar pola organización.

597. As copias de respaldo posuirán o mesmo nivel de seguridade que os datos orixinais no que se refire a integridade, confidencialidade, autenticidade e trazabilidade. En particular, debe considerarse a conveniencia ou necesidade de que as copias de seguridade estean cifradas para garantir a confidencialidade (nese caso estarase ao disposto en [op.exp.11]).

598. Recoméndase establecer un proceso de autorización para a recuperación de información das copias de respaldo.

599. Recoméndase conservar as copias de respaldo en lugar(es) suficientemente independente(s) da localización normal da información en explotación como para que os incidentes previstos na análise de riscos non se dean simultaneamente en ambos lugares, por exemplo, se se conservan na mesma sala utilizar un armario ignífugo.

600. O transporte de copias de respaldo desde o lugar onde se producen ata o seu lugar de almacenamento garante as mesmas seguridades que os controis de acceso á información orixinal.

601. As copias de respaldo deben abarcar:

- información de traballo da organización
- aplicacións en explotación, incluíndo os sistemas operativos
- datos de configuración, servizos, aplicacións, equipos, etc.
- claves utilizadas para preservar a confidencialidade da información

602. Para os puntos anteriores ver [op.exp] e [mp.info.3].

603. O responsable da información debe determinar a frecuencia coa que deben realizarse as copias e o período de retención durante o que mantelas.

604. En caso de dispoñer dun Plan de Continuidade, as copias de seguridade deberán realizarse cunha frecuencia que permita cumprir co RPO e cun obxectivo de tempo de restauración que permita cumprir o RTO.

605. Recoméndase realizar periodicamente probas de restauración de copias de seguridade.

Anexo 2 Cuestionario básico de Ciberseguridade

Anexo 3 Programa de auditoría (fichas de revisión)

Anexo 4. Niveis de madurez dos procesos segundo a Guía de seguridade CCN-STIC 804

Para avaliar os resultados xerais por cada un dos CBCS utilizarase o modelo de nivel de madurez dos procesos[16] 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 presupostos 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 se realizan 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 incrementales 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.*

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

Anexo 5. Tipos de ciberincidentes

O ENS define incidente de seguridade como: Suceso inesperado ou non desexado con consecuencias en detrimento da seguridade do sistema de información.

Na Guía CCN-STIC 817 sinálase que, seguindo a liña terminolóxica iniciada pola Estratexia de Ciberseguridade Nacional, ao longo do citado documento utilizarase o termo ciberincidente como sinónimo de incidente de seguridade no ámbito dos Sistemas de Información e as Comunicacións.

Clasificación dos ciberincidentes segundo a Guía de seguridade CCN-STIC 817

Clase de Ciberincidente	Descrición	Tipo de ciberincidente
Código daniño	Software cuxo obxectivo é infiltrarse ou danar un computador, servidor ou outro dispositivo de rede, sen o coñecemento do seu responsable ou usuario e con finalidades moi diversas.	Virus Vermes Troianos Spyware Rootkit Ransomware (secuestro informático) Ferramenta para Acceso Remoto Remote Access Tools (RAT)
Dispoñibilidade	Ataques dirixidos a poñer fóra de servizo os sistemas, ao obxecto de causar danos na produtividade e/ou a imaxe das institucións atacadas	Denegación [Distribuída] do Servizo DoS / DDoS Fallo (Hardware/Software) Erro humano Sabotaxe
Obtención de información	Ataques dirixidos a solicitar información fundamental que permita avanzar en ataques máis sofisticados, a través de enxeñería social ou de identificación de vulnerabilidades.	Identificación de activos e vulnerabilidades (escaneo) Sniffing Enxeñería social Phishing
Intrusións	Ataques dirixidos á explotación de vulnerabilidades de deseño, de operación ou de configuración de diferentes tecnoloxías, ao obxecto de introducirse de forma fraudulenta nos sistemas dunha organización.	Compromiso de conta de usuario Defacement (desfiguración) Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados Inxección SQL Spear Phishing Pharming Ataque de forza bruta Inxección de Ficheiros Remota Explotación de vulnerabilidade software Explotación de vulnerabilidade hardware Acceso non autorizado a rede
Compromiso da información	Incidentes relacionados co acceso e fuga (Confidencialidade), modificación ou borrado (Integridade) de información non pública.	Acceso non autorizado a información Modificación e borrado non autorizada de información. Publicación non autorizada de información. Exfiltración de información
Fraude	Incidentes relacionados con accións fraudulentas derivadas de suplantación de identidade, en todas as súas variantes.	Suplantación / Spoofing Uso de recursos non autorizado Uso ilexítimo de credenciais Violacións de dereitos de propiedade intelectual ou industrial.

Clase de Ciberincidente	Descrición	Tipo de ciberincidente
Contido abusivo	Ataques dirixidos a danar a imaxe da organización ou a utilizar os seus medios electrónicos para outros usos ilícitos (tales como a publicidade, a extorsión ou, en xeral a ciberdelincuencia).	Spam (Correo Lixo) Acoso/extorsión/ mensaxes ofensivas Pederastia/ racismo/ apoloxía da violencia/delito, etc.
Política de seguridade	Incidentes relacionados por violacións de usuarios das políticas de seguridade aprobadas pola organización.	Abuso de privilexios por usuarios Acceso a servizos non autorizados Sistema desactualizado Outros
Outros	Outros incidentes non incluídos nos apartados anteriores	