

Quèstions prèvies

■ Feedback tallers



ICS > 35 > 35.030

ISO/IEC 27002:2013

Information technology – Security techniques – Code of practice for information security controls

ABSTRACT [PREVIEW](#)

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It is designed to be used by organizations that intend to:

1. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
2. implement commonly accepted information security controls;
3. develop their own information security management guidelines.

FORMAT	LANGUAGE
✓ PDF + COLOR EPUB	English
PDF + EPUB	English
PDF + EPUB + REDLINE	English
PAPER	English

CHF 178 [BUY](#)

Qüestions prèvies

- Feedback tallers

GENERAL INFORMATION

Status :  Published

Publication date : 2013-10

Edition : 2

Number of pages : 80

Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection

ICS : 35.030 IT Security

Quèstions prèvies

■ Feedback tallers

LIFE CYCLE

A standard is reviewed every 5 years



REVISIONS / CORRIGENDA

Previously

ISO/IEC 27002:2005

Now under review

ISO/IEC 27002:2013

Corrigenda/Amendments

ISO/IEC 27002:2013/Cor 1:2014

ISO/IEC 27002:2013/Cor 2:2015

Will be replaced by

ISO/IEC WD 27002

Qüestions prèvies

- Feedback tallers

- Referències

- https://es.wikipedia.org/wiki/ISO/IEC_27000
 - <http://iso.org>
 - https://es.wikipedia.org/wiki/ISO/IEC_27000
 - ...

- Referències

- ISO/IEC 27000, Wikipedia, consulta el 3/10/2019
https://es.wikipedia.org/wiki/ISO/IEC_27000
 - International Standards Organisation, consulta el 3/10/2019
<http://www.iso.org>

Avaluació

- **Per superar el curs**

- Cal assistir 70% sessions presencials / síncrones
- Cal lliurar 70% activitats

- **Nota del curs:**

- 30% mitjana dels tallers
- 50% mitjana dels projectes
- 10% presentació del projecte final
- 10% qüestionaris “soft skills”
- La nota serà A+, A, B, C+, C-, per fer la mitjana es convertirà a números.

Avaluació

- Fareu un qüestionari sobre l'ús de Google Docs i un sobre l'ús de Trello (soft skills) + demostrar que els heu utilitzat.

Avaluació

- **Dubtes sobre el projecte?**



Kali Linux

Organitza:



SOC

Servei d'Ocupació
de Catalunya



Generalitat
de Catalunya



Unió Europea
Fons Social Europeu
L'FSE inverteix en el teu futur

Imparteix:



Universitat
Oberta
de Catalunya

Col·labora:



[PQ]
[TM] Pla de Qualificació en Tecnologia Mòbil

Kali Linux

■ Què és?

- És una distribució de Linux basada en Debian, dissenyada per a auditòries de seguretat, els tests d'intrusió i la informàtica forense.
- És una millora respecte la coneguda BackTrack, la qual no s'actualitza des de 2012.
- Kali s'actualitza de forma freqüent.
- Està gestionada per Offensive Security Ldt, fent servir paquets GPL, per la qual cosa el codi font està disponible.
- El seu desenvolupament es recolza en un reduït grup de desenvolupadors de confiança, que signen els paquets amb GPG per evitar atacs (troians).

Kali Linux

■ ENQUESTA!

- Coneixeu Linux?
- El teniu instal·lat?

Kali Linux

■ On es pot instal·lar?

- En una estació de treball, en un portàtil...
- En un ordinador "small form factor"
- En una Raspberry Pi, en telèfons mòbils, etc. de manera que és fàcil que la màquina passi desapercebuda si ens enduem la Kali per fer auditories de seguretat.
- **En una màquina virtual (VirtualBox, VMWare, Hyper-V)**

Kali Linux

■ Eines que incorpora

■ <http://tools.kali.org/tools-listing>

Kali Linux Tools Listing

Information Gathering

- ace-voip
- Amap
- APT2
- arp-scan
- Automater
- bing-ip2hosts
- braa
- CaseFile
- CDPSnarf
- cisco-torch
- copy-router-config

Vulnerability Analysis

- BBQSQL
- BED
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- copy-router-config
- Doona
- DotDotPwn
- HexorBase
- iSQL_Injection

Wireless Attacks

- Airbase-ng
- Aircrack-ng
- Airdecap-ng and Airdecloak-ng
- Aireplay-ng
- airgraph-ng
- Airmon-ng
- Airodump-ng
- airodump-ng-oui-update
- Airolib-ng
- Airserv-ng
- Airtun-ng

Web Applications

- apache-users
- Arachni
- BBQSQL
- BlindElephant
- Burp Suite
- CutyCapt
- DAVTest
- deblaze
- DIRB
- DirBuster
- fimap

Kali Linux

■ Modes d'arrencada

- Instal·lat en la màquina
- Mode Live
- Mode *forensic*
- *Live USB persistence*
- ...

En Kali hi ha el 'root' amb contrasenya 'toor'.

Kali Linux

■ Demo

- **(1)** Instal·lació sobre VirtualBox
- Actualització de paquets
 - apt-get update
 - apt-get upgrade
 - apt-get dist-upgrade
- **(2)** Exemple d'eina de cerca d'informació
 - **nmap**

<https://www.kali.org/downloads/>

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>. Downloads are **rate limited to 5 concurrent connections**.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 32-Bit	Torrent	2019.3	2.9G	3fdf8732df5f2e935e3f21be93565a113be14b4a8eb410522df60e1c4881b9a0
Kali Linux 64-Bit	Torrent	2019.3	2.9G	d9bc23ad1ed2af7f0170dc6d15aec58be2f1a0a5be6751ce067654b753ef7020
		2019.3	3.5G	dd44391927d38d91cae96ed1a8b918767d38bee2617761fab2d54ad8c77319ec

Kali Linux Custom Image Downloads - Offensive Securi...		The leading operating system for PCs, IoT devices, ser...			Ubuntu - Viquipèdia, l'enciclopèdia lliure	
						
Courses	Certifications	Labs	Pentest	Who We Serve	Pricing	Kali & More.
Kali Linux VirtualBox Images						
Image Name	Torrent	Version	Size	SHA256Sum		
Kali Linux VirtualBox 32-Bit	Torrent	2019.3	3.3G	6aa96ae5f0b6c4bf233a62528954d9c9caa4db255b2da9245950df0c2ff2d2b7		
Kali Linux VirtualBox 64-Bit	Torrent	2019.3	3.4G	1104bd669754ccd9585f504bc7071e04729ce8fb35107d77d2922d3fa469a6f4		



- 1. Nikto
- 2. Yersinia
- 3. SSLyze
- 4. Hydra
- 5. John the Ripper
- 6. mimikatz
- 7. sqlmap
- 8. reaver
- 9. w3af
- 10. nikto
- 11. Wapiti
- 12. wpscan
- 13. mitmproxy
- 14. hping3
- 15. apache-users
- 16. SlowHTTPTest
- 17. cukoo
- 18. xplico
- 19. metasploit
- 20. dnsmap
- 21. Kali nethunter



Seguretat operacional (1)

Organitza:



SOC

Servei d'Ocupació
de Catalunya

Generalitat
de Catalunya



Unió Europea
Fons Social Europeu
L'FSE inverteix en el teu futur

Imparteix:

UOC
Universitat
Oberta de Catalunya

Col·labora:

MOBILE
WORLD CAPITAL.
BARCELONA

[PQ]
[TM]

Pla de
Qualificació en
Tecnologia
Mòbil

Mecanismes de seguretat

Administració de la seguretat

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PDI_08196184



Mecanismes de seguretat

- **Mesures de prevenció**
 - Augmenten la seguretat del sistema durant el seu funcionament.
- **Mesures de detecció**
 - S'utilitzen per a detectar violacions de la seguretat d'un sistema.
- **Mesures de recuperació**
 - Permeten la recuperació del funcionament correcte del sistema una vegada s'ha produït l'atac.

Seguretat de l'entorn

■ Els servidors

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.
- Mantenir els dispositius d'emmagatzematge en un lloc diferent de la resta de maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic.
- Protegir i aïllar cablatge de xarxa (tant per protegir-los de danys físics com de l'espionatge).
- Instal·lació de càmeres de vídeo vigilància
- Sistemes anti-incendi, HVAC, SAI, etc.

Seguretat de l'entorn

■ Estacions de treball

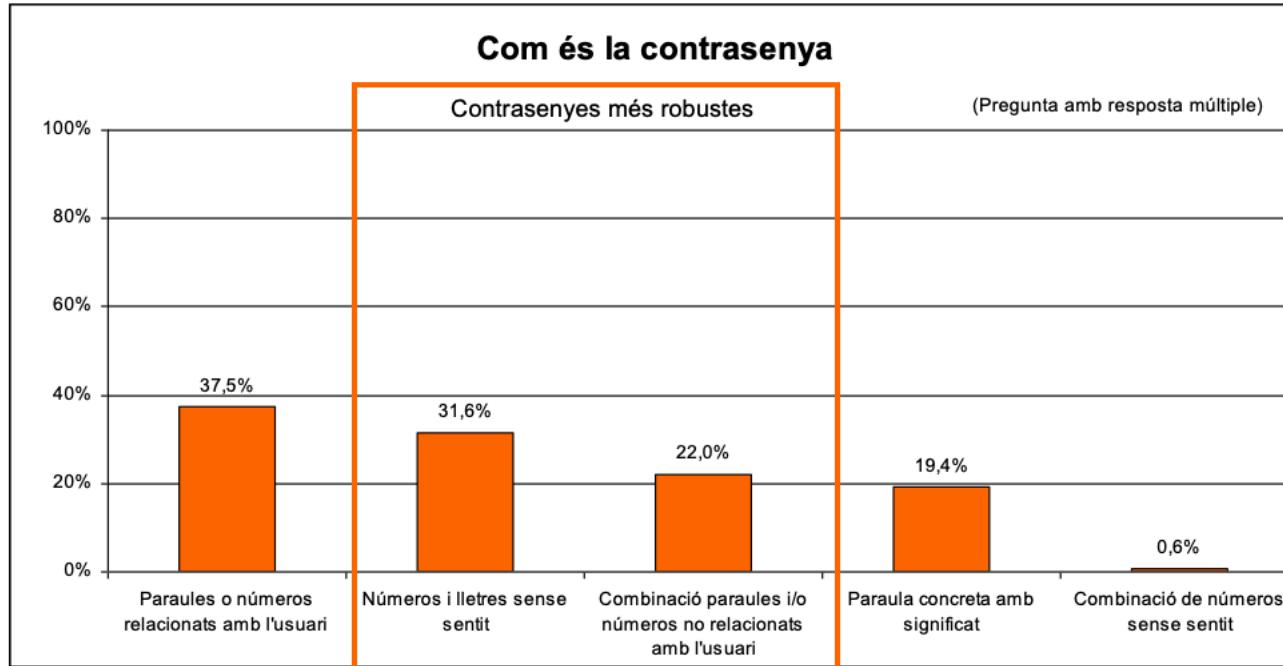
- Ús de contrasenyes en els protectors de pantalla.
- Utilització de contrasenyes de BIOS.
- Desactivar les opcions d'autocompletar i recordar contrasenyes dels navegadors d'internet.
- Actualitzacions del sistema operatiu i de programari.
- Sistemes d'autenticació d'usuaris

Seguretat de l'entorn

- Sistemes d'autenticació d'usuaris
 - Basats en allò que es coneix (contrasenyes)
 - No escriure la contrasenya
 - Canviar-la periòdicament
 - No repetir-la en comptes diferents
 - Evitar introduir-la en presència d'altres persones
 - No compartir-la
 - Evitar paraules de diccionari
 - Evitar utilitzar dades que poden ser conegudes per altres personnes
 - Mínim vuit caràcters, amb números, caràcters especials.
 - Bona política: fer servir mnemotècnics.

- **Contrasenyes**

- Un 53,6% de les contrasenyes dels enquestats són robustes: es consideren robustes aquelles formades per números i lletres sense sentit, o bé per una combinació de paraules o números no relacionats amb l'usuari.



Seguretat de l'entorn

- Sistemes d'autenticació d'usuaris
 - Basats en allò que es té (tokens, smart cards)
 - Basats en allò que s'és (biometria)
 - Empremta dactilar
 - Reconeixement facial
 - Patrons de la retina o l'iris

Seguretat de l'entorn

■ Malware o codi maliciós

- Qualsevol fitxer que resulti perniciós per a un sistema informàtic.
- A vegades es pot inserir dins un programa "autoritzat".
- Sovint pot estar ocult i provocar tota mena de danys.
- Antivirus de mentida.

Seguretat de l'entorn

- Programari amb errors de programació
 - Vulnerabilitats o *exploits*
 - És fonamental estar al dia de tots els forats de seguretat que presenta el nostre programari mitjançant una subscripció a fòrums sobre seguretat informàtica.
- Eines de seguretat mal emprades
 - Escàners, programari per atacar contrasenyes, eines d'auditoria (Kali), etc.

Seguretat de l'entorn

■ Bombes lògiques

- Parts del codi d'un programari que es manté inert fins que no es produeix una certa condició que l'activa (una data, una seqüència de tecles, etc.)
- Alguns programadors maliciosos insereixen aquestes parts del codi en els seus programaris amb la intenció d'activar-les si són acomiadats de la organització que treballen.

■ *Backdoors*

- Són portes d'entrada a sistemes operatius i programaris, inserides pels mateixos dissenyadors o programadors, que els permeten d'accedir a l'aplicació i evitar tots els mecanismes d'autenticació.

Seguretat de l'entorn

■ Virus

- Habitualment, els virus són seqüències de codi que s'insereixen en un fitxer executable (anomenat hoste) de manera que quan s'executa també ho fa el virus.
- La principal qualitat és l'autoreplicació, és a dir, la capacitat d'inserir-se en altres programaris del sistema informàtic atacat. Poden tenir efectes summament destructius (o simplement perseguir la replicació): format d'un disc dur, esborrament de fitxers, disminució del rendiment del sistema, etc. Els virus constitueixen un dels problemes de codi maliciós més importants en sistemes informàtics basats en Windows.

Seguretat de l'entorn

■ Cucs

- Similars al virus, un cuc és un programa que és capaç d'autoexecutar-se amb la finalitat de propagar-se per la xarxa i col·lapsar l'amplada de banda dels sistemes atacats o danyar-ne els ordinadors (poden anar acompanyats de virus).

Seguretat de l'entorn

■ Troians

- Són parts de codi inserides en el programari que habitualment s'utilitza en el sistema. Aquest codi es manté ocult i duu a terme tasques diverses sense que l'usuari o l'administrador se n'adonin. Camuflat sota l'aparença d'un programari útil o habitual, no solen ocasionar efectes destructius.
- Generalment capturen contrasenyes i altres dades confidencials i les envien per correu electrònic a la persona que ha introduït el troià dins el sistema atacat. També poden obrir forats de seguretat que posteriorment podran ser aprofitats per l'atacant. Realment, els efectes dels troians poden arribar a ser molt perniciosos i el seu ús pot ser font de delictes. Per exemple, mitjançant un troià és possible activar remotament una càmera web (webcam) i gravar l'usuari destí amb total desconeixement per part d'aquest.

Seguretat de l'entorn

■ *Phishing*

- Pràcticament tots els usuaris d'Internet hem hagut de patir la recepció de correus electrònics que, fent-se passar com a “fiables” i procedents d'entitats bancàries reals, ens sol·liciten informació confidencial que una veritable entitat bancària mai sol·licitaria a través del correu electrònic. Els links o vincles d'aquests correus ens remeten a llocs web falsos i que no corresponen a l'entitat bancària real.

■ *Hoax*

- Un correu electrònic en què s'avisa de l'existència de virus (naturalment falsos) d'efectes devastadors contra els quals no existeix cap antivirus que els pugui detectar.

Seguretat de l'entorn

- *Adware*
 - És un programari que mostra publicitat diversa. Habitualment s'instal·la sense el consentiment de l'usuari.
- *Spyware o programari espia*
 - És un programari que envia dades a empreses sobre els nostres hàbits d'Internet. Com de costum, solen instal·lar-se sense el permís de l'usuari. Hi ha múltiples solucions per a “netejar” els nostres sistemes d'aquesta mena de programaris.

Atacs de denegació de servei

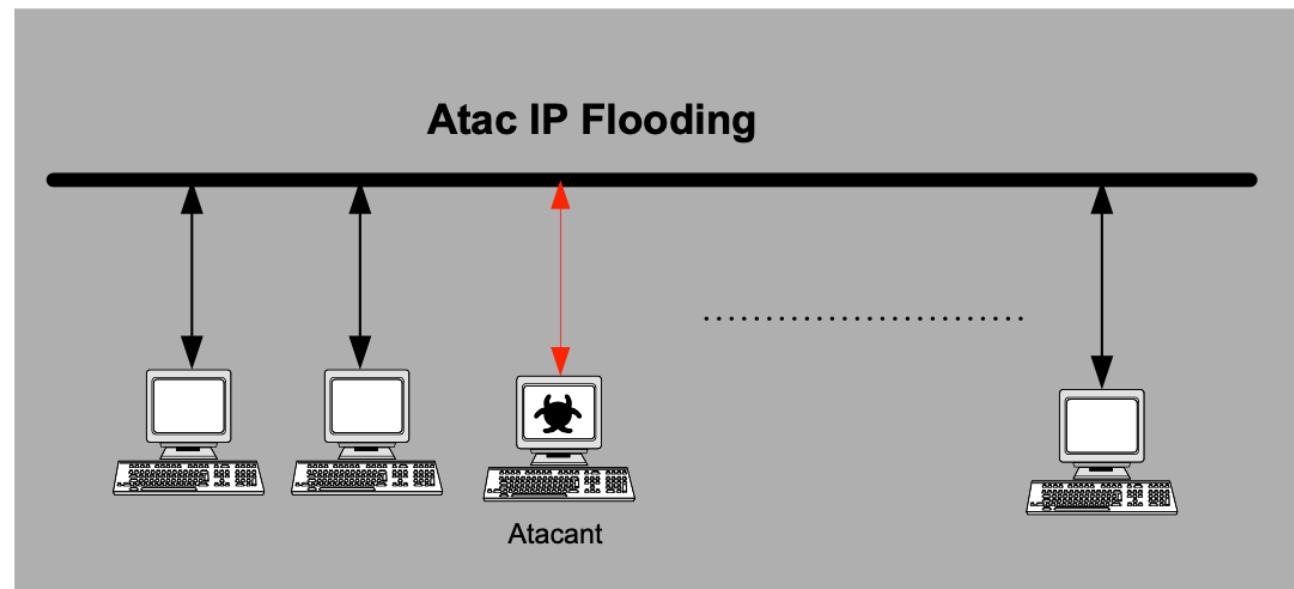
- Tota acció iniciada per una persona o per altres causes, que inutilitza el maquinari i/o programari, de manera que els recursos del sistema no siguin accessibles des de la xarxa.
- Poden arribar a implicar milers d'ordinadors intermediaris (*zombies* en una *botnet*).

Atacs de denegació de servei

■ IP flooding

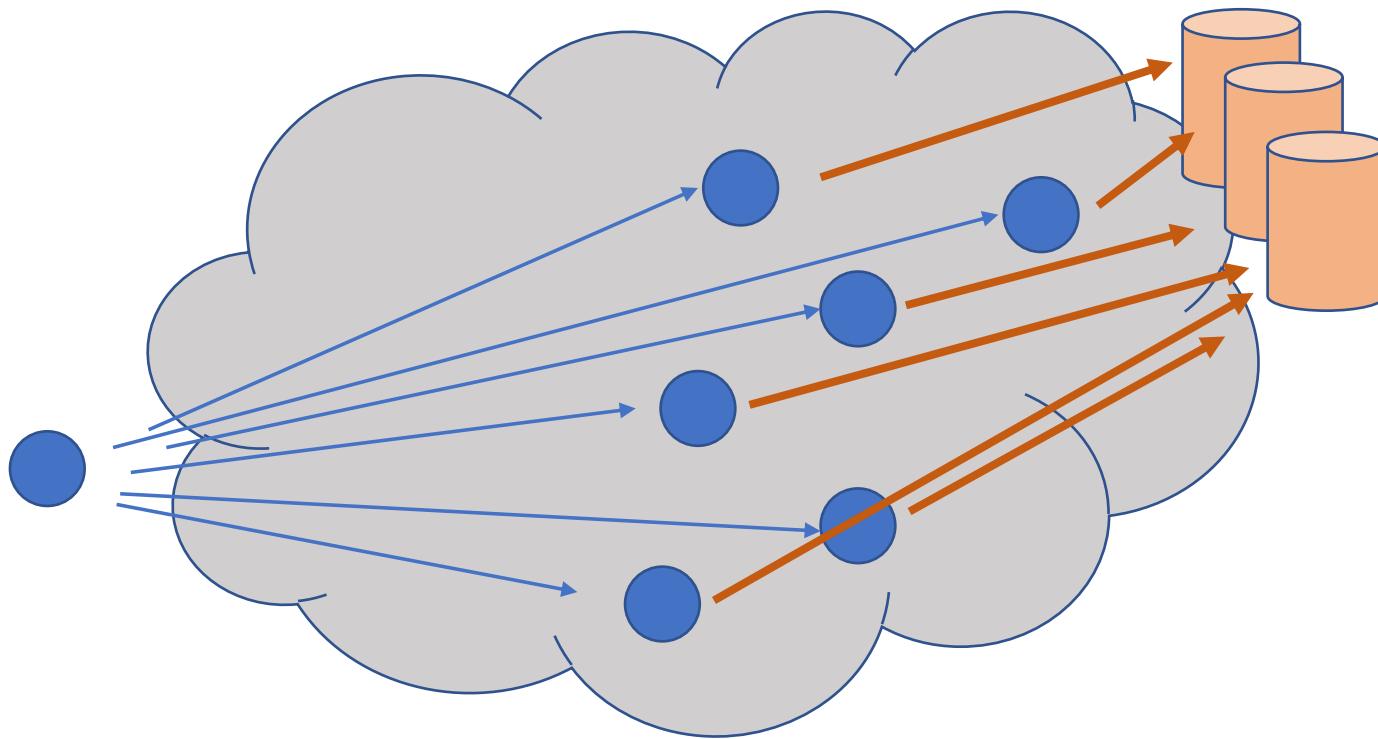
Aquest atac es realitza habitualment en xarxes locals o en connexions amb una gran amplada de banda. Consisteix en la generació de trànsit d'escombraries amb l'objectiu d'aconseguir la degradació del servei. D'aquesta forma, es redueix l'amplada de banda disponible i s'alenteixen les comunicacions existents de tota la xarxa.

Aquest tipus d'atac es dóna principalment en xarxes locals on el control d'accés al medi és nul i qualsevol màquina pot enviar i rebre paquets sense que s'estableixi cap tipus de limitació en l'amplada de banda que consumeix.



Atacs de denegació de servei

- IP flooding



Atacs de denegació de servei

■ Atac SYN

Aquest atac consisteix en l'enviament, per part del sistema atacant, d'un gran nombre de sol·licituds de connexió per segon. El sistema atacat respon correctament les sol·licituds de connexió, però en no obtenir resposta del sistema atacant, es col·lapsa i no pot atendre les sol·licituds de connexió legítimes. Aquest atac es basa en el *modus operandi* del protocol d'establiment de sessió entre client i servidor (vegeu la figura):

- 1) L'ordinador client envia una sol·licitud de sincronització (SYN) al servidor.
- 2) El servidor respon amb un missatge ACK (*acknowledgement*) i un missatge de sincronització al client.
- 3) En resposta a la sol·licitud de sincronització, l'ordinador client envia una resposta ACK al servidor.

Atacs de denegació de servei

Quan un atacant configura una inundació de paquets SYN de TCP, no té cap intenció de completar el protocol d'intercanvi i establir la connexió. El seu objectiu és excedir els límits establerts pel nombre de connexions que estan a l'espera de ser establertes per a un servei donat.

Això pot fer que el sistema que és víctima de l'atac sigui incapàç d'establir qualsevol connexió addicional per a aquest servei fins que les connexions que estan a l'espera baixin del llindar.

Fins que s'arriba a aquest límit, cada paquet SYN genera un SYN/ACK que romandrà a la cua (que és generalment d'entre 5 i 10 connexions) a l'espera d'establir-se. És a dir, cada connexió té un temporitzador, un límit per al temps que el sistema espera l'establiment de la connexió, que tendeix a configurar-se en un minut.

Atacs de denegació de servei

Quan s'excedeix el límit de temps, s'allibera la memòria que manté l'estat d'aquesta connexió i el compte de la cua de serveis disminueix en una unitat. Després d'assolir el límit, pot mantenir-se completa la cua de serveis, evitant que el sistema estableixi noves connexions en aquest port amb uns 10 nous paquets SYN per minut.

Com que l'únic propòsit de la tècnica és inundar la cua, no té cap sentit utilitzar l'adreça IP real de l'atacant, ni tampoc retornar els SYN/ACK, ja que d'aquesta forma facilitaria que algú pogués arribar fins a ell seguint la connexió. Per tant, normalment es falseja l'adreça d'origen del paquet, modificant per a això la capçalera IP dels paquets que intervindran en l'atac d'una inundació SYN.

Atacs de denegació de servei

- Notícies sobre atacs de denegació de servei
 - https://elpais.com/tecnologia/2018/03/05/actualidad/1520249257_684529.html

Así se ha producido el mayor ataque DDoS de la historia

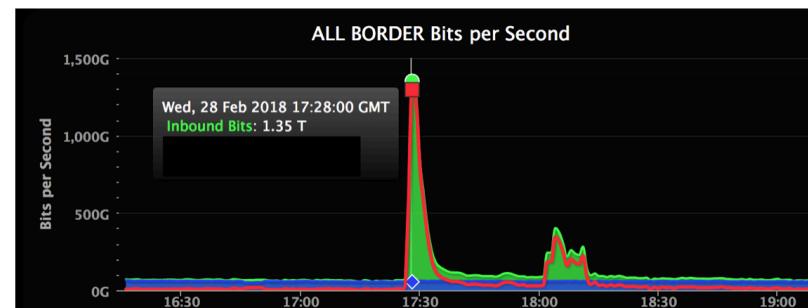
GitHub logra resistir una embestida sin precedentes



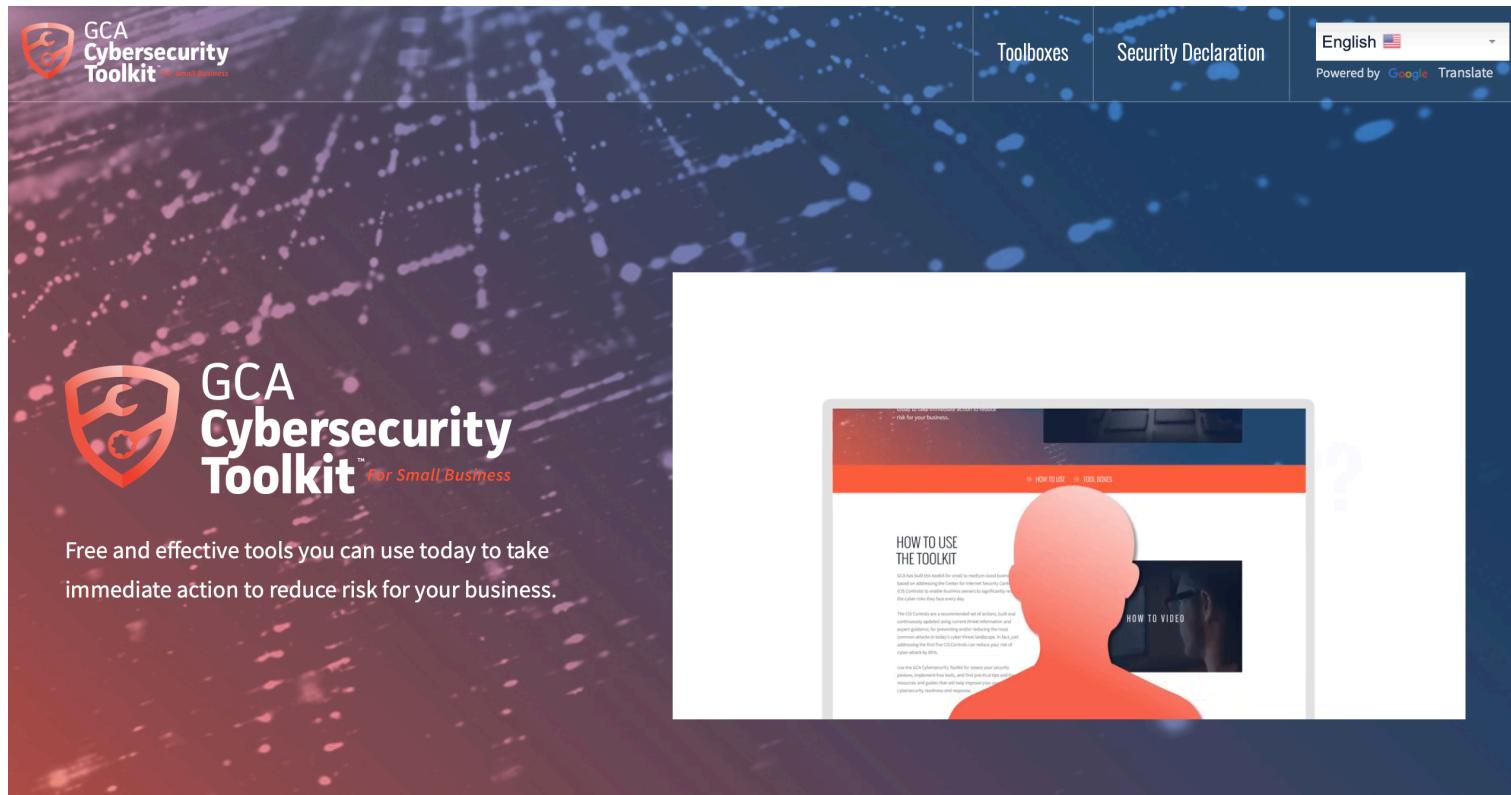
JOSÉ MENDIOLA ZURIARRAIN

5 MAR 2018 - 16:03 CET

<https://techcrunch.com/2018/03/02/the-worlds-largest-ddos-attack-took-github-offline-for-less-than-tens-minutes/>



■ Global Cybersecurity Alliance



■ Global Cybersecurity Alliance





ISE TIC

Índex de Seguretat de l'Empresa en relació a les TIC

Estudi sobre la seguretat de la informació a les empreses 2010

Amb la col·laboració de:



UNIVERSITAT ROVIRA I VIRGILI

Juny de 2010



1. Objectiu

- **Objectiu**
 - L'**Índex de Seguretat de l'Empresa en relació a les TIC** (d'ara endavant **ISE TIC**) és un valor numèric que té com a objectius:
 - Comparar la seguretat TIC entre diferents empreses
 - Analitzar l'evolució temporal de la seguretat TIC en les empreses, a partir de successius estudis i càlculs de l'ISE TIC
 - El valor de l'ISE TIC i altres índexs complementaris és al rang **[0,10]**

2. Metodología



2. Metodologia

- **S'utilitzen 30 indicadors recollits en el treball de camp**
- **Té en compte indicadors de 5 àmbits**
 - **Gestió d'identitat i accés.** Com s'accedeix als equips informàtics i com es gestiona la identitat de llurs usuaris.
 - **Seguretat en l'equip de treball.** Anàlisi de la seguretat dels ordinadors amb què els treballadors i treballadores duen a terme llurs activitats.
 - **Seguretat en aplicacions i dades.** Factors relacionats amb els documents electrònics i la seva gestió.
 - **Seguretat a la xarxa.** Control i gestió de la seguretat en l'ús de la xarxa.
 - **Estructura i organització.** Aspectes relacionats amb les polítiques de seguretat TIC de l'empresa, i la relació dels treballadors envers la seguretat TIC.

Aquesta distribució es basa en el que es recomana al document *Taxonomía de Soluciones de Seguridad TIC*, INTECO, 2a edició, 2009



2. Metodologia

- **Té en compte dos nivells d'indicadors**
 - **Crítics.** Són aquells que, cas de ser evaluats negativament, comporten una clara falla en la seguretat que afecta al globalment al sistema.
 - **No crítics.** Es consideren essencials per a la seguretat de l'empresa però que en cas de ser evaluats negativament no afecten a la seguretat global de sistema.



2. Metodologia

- Nombre i tipus d'indicadors**

- La següent taula mostra el nombre d'indicadors segons l'àmbit i el nivell:

Àmbit	Crític	No crític	Total
Gestió d'identitat i accés	3	2	5
Seguretat en l'equip de treball	3	8	11
Seguretat en aplicacions i dades	0	4	4
Seguretat a la xarxa	1	2	3
Estructura i organització	4	3	7
Total	11	19	30



2. Metodologia

- Indicadors ‘Gestió d’identitat i accés’**

Indicador	Observació	Nivell
Els treballadors s’identifiquen amb un nom d’usuari a l’equip de treball	La identificació única dels treballadors realitzada en el moment d’inici de la sessió de treball, permet analitzar les tasques realitzades pels treballadors de forma individual i detectar possibles mals hàbits o riscos per a la seguretat.	Crític
Els equips de treball disposen de control d'accés amb contrasenya	La utilització de contrasenyes permet restringir l'accés als equips de treball. Això redueix els accessos no autoritzats al sistema. A més també s'incrementen les possibilitats de realitzar un control sobre les tasques i hàbits dels usuaris.	Crític
La contrasenya és robusta (lletres i números sense sentit aparent, longitud 8 o més)	És altament recomanable que les contrasenyes siguin robustes ja que, altrament podria resultar senzill que usuaris no autoritzats accedissin als equips de treball suplantant la identitat d'altres treballadors.	No crític
Es força o demana un canvi de contrasenya com a mínim un cop cada tres mesos	Mantenir la mateixa contrasenya durant llargs períodes de temps augmenta les possibilitats que aquesta contrasenya sigui robada o filtrada a usuaris no autoritzats. Per tant resulta important actualitzar les contrasenyes de forma sistemàtica.	No crític
Ningú a l'empresa coneix totes les contrasenyes	Per tal de permetre una correcta monitorització de les activitats dels treballadors, cal que aquests es puguin identificar de forma única. La compartició de les contrasenyes limita aquesta monitorització perquè permet la suplantació d'identitats. Cal doncs evitar aquesta pràctica.	Crític



2. Metodologia

- Indicadors ‘Seguretat en l’equip de treball’ (1/2)**

Indicador	Observació	Nivell
L’equip de treball no es pot usar en l’àmbit particular	Les activitats que es realitzen en l’àmbit particular sovint difereixen de les que es realitzen en l’àmbit laboral. A més els sistemes de seguretat presents a l’entorn laboral sovint no hi són en el particular. En conseqüència, pot resultar perillós disposar d’un equip de treball amb dades confidencials (de l’empresa) per a l’ús particular.	No crític
L’equip de treball no es pot usar per emmagatzemar informació particular	Informació personal com ara texts, fotografies, vídeos i música, que s’introduceix en els equips de treball mitjançant dispositius externs (no segurs) pot conduir a la creació de forats de seguretat en els equips de treball. És recomanable minimitzar o prohibir l’emmagatzematge d’informació personal a l’equip de treball.	No crític
El sistema operatiu està actualitzat	L’actualització del sistema operatiu resulta vital per evitar atacs que aprofiten vulnerabilitats del sistema. La no actualització del sistema operatiu pot comportar greus riscos de seguretat.	No crític
Els equips de treball disposen d’antivirus	Els virus informàtics són comuns. Podem trobar-los en pàgines web, arxius adjunts als correus electrònics, etc. Disposar d’un sistema de detecció de virus és altament recomanable ja que redueix dràsticament el risc d’infecció.	Crític
Els antivirus estan actualitzats	Els arxius de definició de virus dels antivirus s’han d’actualitzar periòdicament perquè apareixen nous virus diàriament. No actualitzar l’antivirus pot resultar tant perillós com no tenir-ne.	Crític
Els equips de treball disposen de protecció contra programari maliciós	De forma similar als virus, el programari maliciós està present en pàgines web, arxius adjunts als correus, etc. Cal disposar de protecció contra programari maliciós per tal de reduir les possibilitats d’infecció.	No crític
Les eines de protecció envers programari maliciós estan actualitzades	Cal disposar d’una base de dades de programari maliciós actualitzada. Altrament els sistemes de protecció redueixen en gran mesura la seva efectivitat i poden resultar inútils en front de nous perills.	No crític



2. Metodologia

- Indicadors ‘Seguretat en l’equip de treball’ (2/2)**

Indicador	Observació	Nivell
Els equips de treball disposen de tallafocs	Els tallafocs permeten evitar atacs provinents de la xarxa. La seva tasca principal és permetre la comunicació a través de diversos ports (canals de comunicació) i evitar-la a través d'altres. Mitjançant aquesta eina es pot controlar les comunicacions entrants i sortints, augmentant així la seguretat dels equips de treball.	No crític
Els usuaris no poden connectar dispositius externs de memòria a l'equip de treball	La connexió de dispositius externs (no segurs) a l'equip de treball permet evitar els controls d'accés presents a la xarxa internar/externa. Això pot provocar l'entrada inadvertida de programari maliciós i virus.	No crític
Els usuaris no disposen de permís il·limitat a l'equip de treball per instal·lar programes	La instal·lació programari inadequat pot significar un risc per a les dades emmagatzemades a l'equip de treball o a la pròpia xarxa interna. És desitjable que únicament usuaris autoritzats instal·lin el software necessari per a cada equip de treball.	Crític
Els usuaris no disposen de permís il·limitat en l'ús de la xarxa (execució eMule, messenger, skype...)	L'execució indiscriminada de qualsevol mena de programari pot resultar perillosa. Utilitzar programari de compartició d'arxius com eMule pot provocar la infecció dels equips de treball i la conseqüent pèrdua d'informació i temps. Resulta desitjable evitar que usuaris inexperts disposin de permís il·limitat per accedir a la xarxa.	No crític



2. Metodologia

- Indicadors ‘Seguretat en aplicacions i dades’**

Indicador	Observació	Nivell
S'utilitzen avisos sobre seguretat i privadesa al final del text del correu electrònic	Donat que existeix la possibilitat de que un determinar missatge s'envii per error a un destinatari no autoritzat, resulta necessari afegir una nota informativa al peu dels correus que continguin dades de caràcter confidencial. Aquesta és una mesura legal més que no pas tècnica.	No crític
Es fa una còpia de seguretat dels documents de treball com a mínim un cop per setmana	La realització sistemàtica de còpies de seguretat redueix dràsticament el risc de pèrdua d'informació en cas de fallides.	No crític
L'accés als fitxers que contenen dades de caràcter personal (clients, proveïdors, etc.) està restringit	En compliment de la llei orgànica de protecció de dades, cal restringir l'accés a les dades de caràcter personal.	No crític
Les dades de caràcter personal (clients, proveïdors, etc.) es desen de forma xifrada	En compliment de la llei orgànica de protecció de dades, cal xifrar les dades de caràcter personal.	No crític



2. Metodologia

- Indicadors ‘Seguretat a la xarxa’**

Indicador	Observació	Nivell
Els treballadors no poden connectar a la xarxa dispositius personals (p.ex. Portàtils, pda)	De forma similar a la connexió de dispositius d'emmagatzematge de dades a les estacions de treball, la connexió de dispositius personals a la xarxa interna de l'empresa pot provocar la propagació de riscos de seguretat (virus, programari maliciós). Cal, doncs, evitar-ho.	No crític
La xarxa wifi té control d'accés	Les connexió a una xarxa wifi no pot ser controlada mitjançant limitacions físiques, ja que l'accés és sense fils. Per tal de garantir una correcta utilització de la xarxa i evitar accessos no autoritzats a la xarxa interna de l'empresa, cal controlar l'accés a la xarxa wifi mitjançant contrasenya (o similar).	Crític
Existeix un control de tràfic entre la xarxa externa (p.ex. Internet) i la interna	Tot i que la xarxa interna estigui protegida i controlada, si no es vigila el tràfic de dades provenint d'Internet, poden aparèixer riscos de seguretat a la xarxa interna que poden provocar la pèrdua de dades i temps.	No crític



2. Metodologia

- Indicadors ‘Estructura i organització’**

Indicador	Observació	Nivell
Els sistemes de seguretat de l'empresa són gestionats per experts	La seguretat TIC és un tema prou important com per que la seva gestió sigui a càrrec d'experts.	Crític
L'empresa disposa d'alguna política de seguretat TIC	Les empreses han de disposar d'unes normes i regles pel que fa al bon ús de la xarxa, Internet i els equips informàtics.	Crític
Tots els treballadors no disposen dels mateixos permisos/privilegis en l'accés als equips	La distribució heterogènia de permisos/privilegis d'accés als equips permet limitar l'accés d'usuaris inexperts a equips delicats alhora que permet la seva administració per part de personal qualificat.	No crític
Tots els treballadors no disposen dels mateixos permisos/privilegis en l'accés a les dades	La distribució heterogènia de permisos/privilegis d'accés a les dades permet definir criteris de visibilitat que ajuden a garantir un tracte privat de dades confidencials. És un sistema típicament utilitzat en bases de dades.	Crític
Es realitzen auditories de seguretat informàtica	Convé que les empreses passin revisions pel que fa a la seguretat dels seus equip i l'ús que en fa el personal de l'empresa	No crític
Existeix una política d'actualitzacions per als equips de treball	Convé que les actualitzacions es facin de forma planificada i tenint en compte tots els equips informàtics de l'empresa.	No crític
L'empresa informa als treballadors de les seves polítiques de seguretat TIC	Cas d'haver polítiques de seguretat, els treballadors n'han d'estar al corrent.	Crític



2. Metodologia

- **Càlcul de l'ISE TIC**

- Per a un valor inicial $I = 0$
- S'avalua l'assoliment de cada indicador
 - Si l'indicador és **crític** i l'empresa **l'assoleix**, se **suma 2** a I .
 - Si l'indicador és **no crític** i l'empresa **l'assoleix**, se **suma 1** a I .
 - Si l'indicador és **crític** i l'empresa **no assoleix**, es **resta 2** a I .
 - Si l'indicador és **no crític** i l'empresa **no l'assoleix**, no es suma res.
- I es converteix per tal que ISE TIC $\in [0, 10]$
- En funció de la distribució dels resultats, s'han considerat 5 nivells
 - **Molt insegura** (0 a 2), **insegura** (2.1 a 4), **poc segura** (4.1 a 6), **segura** (6.1 a 8), **molt segura** (8.1 a 10).



2. Metodologia

- Índexs d'àmbit
 - Són valors que descriuen l'assoliment dels indicadors **crítics i bàsics** dels àmbits següents
 - Gestió d'identitat i accés: **ISE TIC_{IA}** (5 indicadors)
 - Seguretat en l'equip de treball: **ISE TIC_{ET}** (11 indicadors)
 - Seguretat en aplicacions i dades: **ISE TIC_{AD}** (4 indicadors)
 - Seguretat a la xarxa: **ISE TIC_{SX}** (3 indicadors)
 - Estructura i organització: **ISE TIC_{EO}** (7 indicadors)
 - Aquests valors també es converteixen per ser dins el rang [0,10]



2. Metodologia

- **Indicador de maduresa en gestió de la seguretat**
 - Valor d'1 a 4 basat, a grans trets, en el model *Capability Maturity Model*:

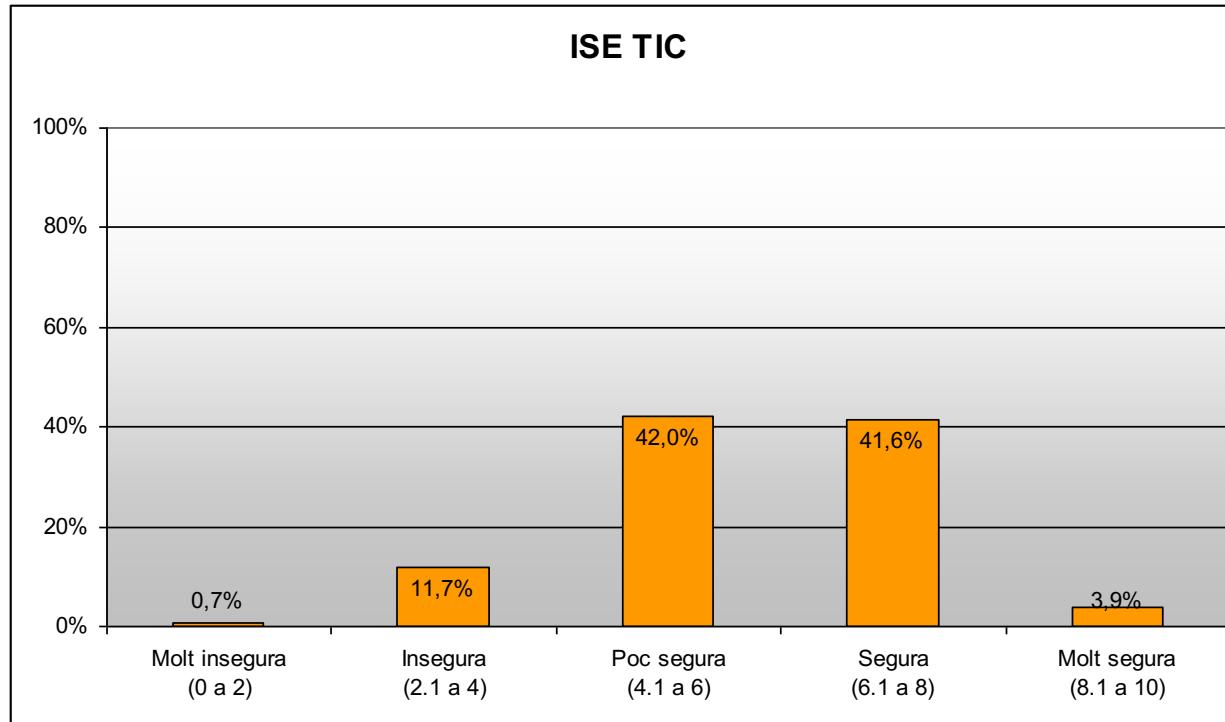
Si l'indicador es compleix	S'assigna el nivell
Es realitzen auditories de seguretat informàtica	4
Els sistemes de seguretat de l'empresa són gestionats per experts	3
L'empresa informa als treballadors de les seves polítiques de seguretat TIC	2
L'empresa disposa d'alguna política de seguretat TIC	1

- Es veurà com evolucionen els diferents índexs en funció d'aquest indicador de maduresa.



3. Resultats: ISE TIC

- ISE TIC

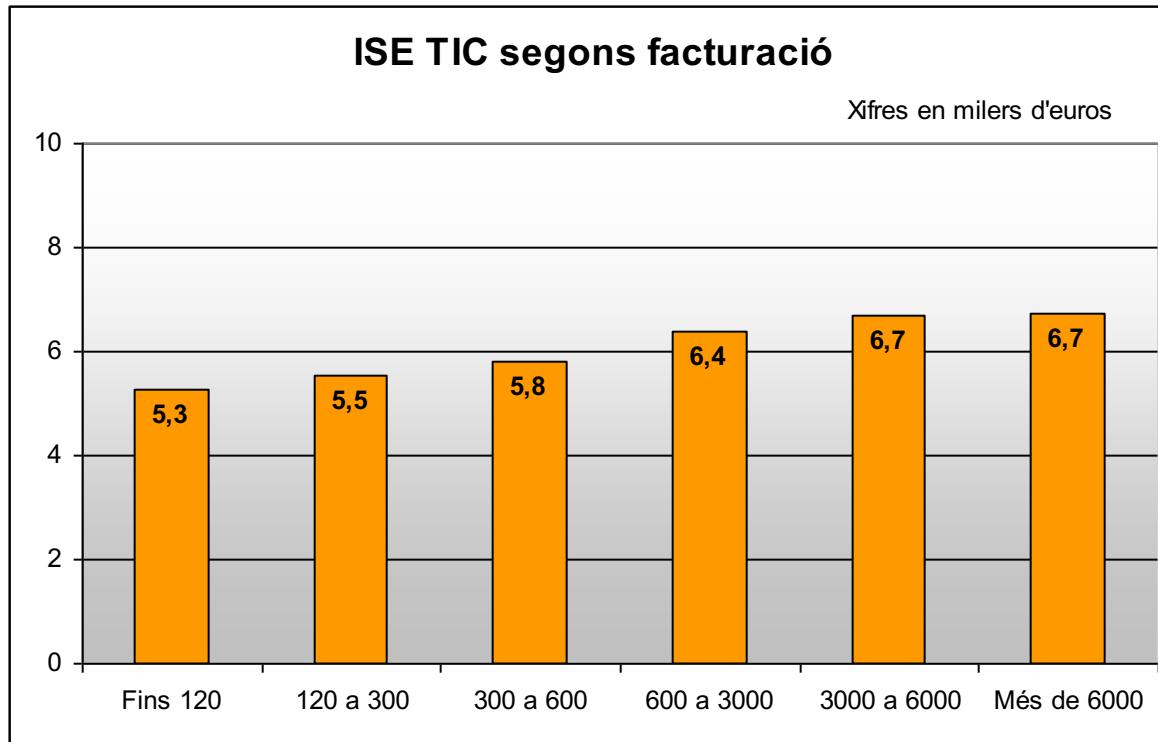


Hi ha dos grups majoritaris: una part considerable de les empreses disposa d'un valor considerat poc segur (42.0%), mentre que una part similar té un nombre acceptable (41.6%) d'indicadors bàsics o crítics assolits.



3. Resultats: ISE TIC

- ISE TIC / Nivell de facturació

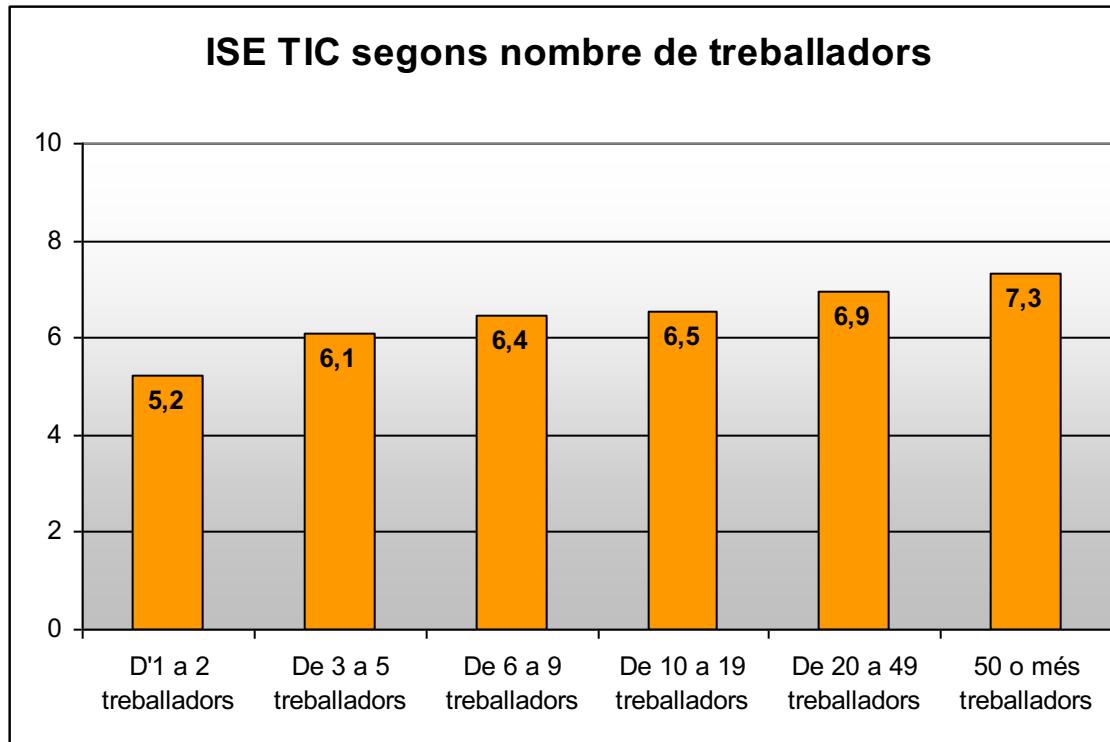


Hi ha una relació clara entre el valor de l'índex i la facturació de l'empresa. A més facturació, valor més gran de l'índex, llevat del darrer interval.



3. Resultats: ISE TIC

- ISE TIC / Nombre de treballadors

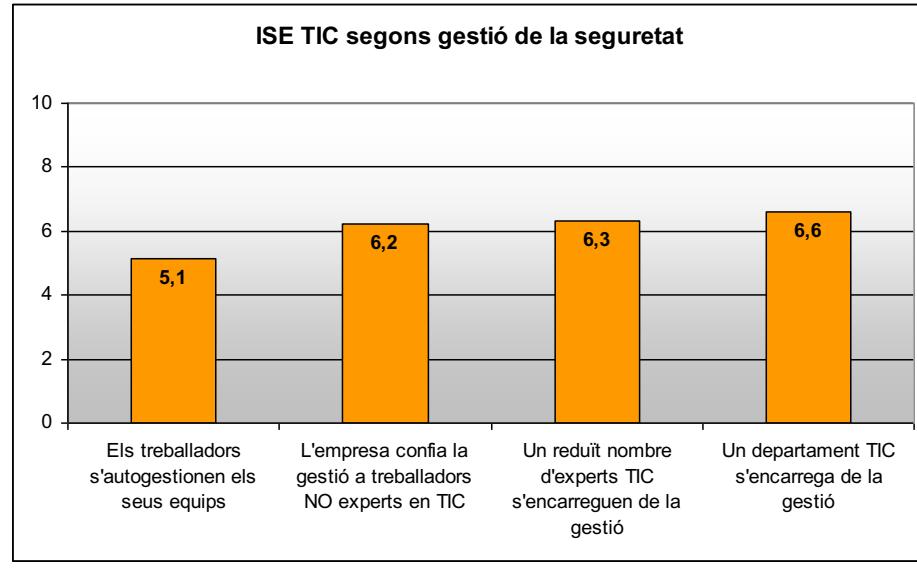
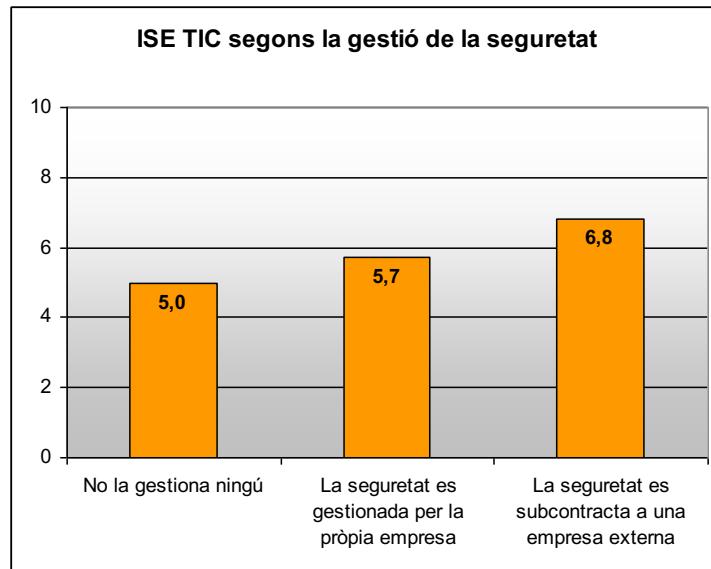


Hi ha una relació clara entre el valor de l'índex i el nombre de treballadors de l'empresa. Com més treballadors, més assolits estan els indicadors de seguretat.



3. Resultats: ISE TIC

- ISE TIC / Gestió de la seguretat**

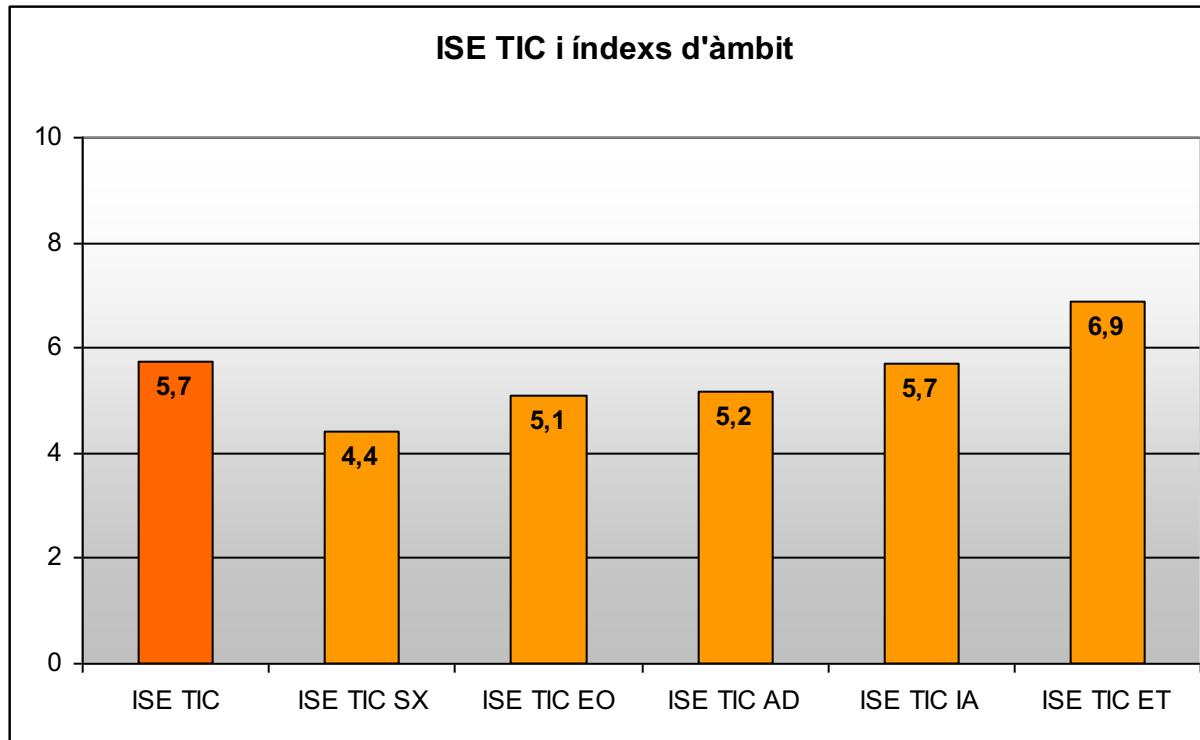


L'índex està clarament relacionat amb la manera com l'empresa gestiona la seguretat. Si aquesta és gestionada per una empresa externa, l'índex és clarament millor que si no la gestiona ningú. Si la pròpia empresa gestiona la seguretat, l'índex millora en funció de la qualificació dels qui la gestionen. En aquest sentit hi ha diferències entre l'autogestió per part dels treballadors i la gestió per part d'un departament TIC. Tanmateix, si hi ha un nombre de treballadors que gestiona la seguretat, no s'aprecien diferències significatives en funció de si aquests són experts TIC o no.



4. Resultats: índexs d'àmbit

- Índexs d'àmbit: resultats globals



Per àmbits, el de seguretat en l'equip de treball és el que presenta, clarament, millors resultats. L'àmbit d'identitat i accés també presenta un bon valor, però no tan elevat com l'anterior. L'àmbit amb un índex més baix és el de seguretat a la xarxa.



5. Altres resultats

- Assoliment d'indicadors**

Els 5 indicadors més assolits	Nivell	% compleix
Els equips de treball disposen d'antivirus	Crític	98,2%
Els antivirus estan actualitzats	Crític	95,8%
Existeix una política d'actualitzacions per als equips de treball	No crític	94,0%
La xarxa wifi té control d'accés (*)	Crític	93,0%
El sistema operatiu està actualitzat	No crític	91,7%

Els 5 indicadors menys assolits	Nivell	% compleix
Els usuaris no disposen de permís il·limitat a l'equip de treball per instal·lar programes	Crític	20,0%
Es força o demana un canvi de contrasenya com a mínim un cop cada tres mesos	No crític	19,0%
Els usuaris no poden connectar dispositius externs de memòria a l'equip de treball	No crític	18,9%
Existeix un control de tràfic entre la xarxa externa i la interna	No crític	16,7%
La contrasenya és robusta	No crític	10,7%



5. Altres resultats

- **Assoliment d'indicadors (1/2)**

Indicador	Nivell	% compleix
Els equips de treball disposen d'antivirus	Crític	98,2%
Els antivirus estan actualitzats	Crític	95,8%
Existeix una política d'actualitzacions per als equips de treball	No crític	94,0%
La xarxa wifi té control d'accés (*)	Crític	93,0%
El sistema operatiu està actualitzat	No crític	91,7%
L'empresa disposa d'alguna política de seguretat TIC	Crític	83,9%
Els equips de treball disposen de tallafocs	No crític	83,2%
Els equips de treball disposen de protecció contra programari maliciós	No crític	80,5%
Els equips de treball disposen de control d'accés amb contrasenya	Crític	79,7%
Els treballadors s'identifiquen amb un nom d'usuari a l'equip de treball	Crític	79,7%
Les eines de protecció envers programari maliciós estan actualitzades	No crític	77,8%
Es fa una còpia de seguretat dels documents de treball com a mínim un cop per setmana	No crític	69,6%
L'equip de treball no es pot usar en l'àmbit particular	No crític	62,8%
S'utilitzen avisos sobre seguretat i privadesa al final del text del correu electrònic	No crític	61,9%
Els usuaris no disposen de permís il·limitat en l'ús de la xarxa	No crític	56,0%
Els sistemes de seguretat de l'empresa són gestionats per experts	Crític	53,0%



5. Altres resultats

- Assoliment d'indicadors (2/2)**

Indicador	Nivell	% compleix
L'accés als fitxers que contenen dades de caràcter personal està restringit	No crític	51,1%
Els treballadors no poden connectar a la xarxa dispositius personals	No crític	50,9%
L'equip de treball no es pot usar per emmagatzemar informació particular	No crític	49,3%
Tots els treballadors no disposen dels mateixos permisos/privilegis en l'accés a les dades	Crític	44,9%
Tots els treballadors no disposen dels mateixos permisos/privilegis en l'accés als equips	No crític	36,0%
Ningú a l'empresa coneix totes les contrasenyes	Crític	32,0%
Les dades de caràcter personal es desen de forma xifrada	No crític	24,4%
Es realitzen auditories de seguretat informàtica	No crític	22,9%
L'empresa informa als treballadors de les seves polítiques de seguretat TIC	Crític	21,5%
Els usuaris no disposen de permís il·limitat a l'equip de treball per instal·lar programes	Crític	20,0%
Es força o demana un canvi de contrasenya com a mínim un cop cada tres mesos	No crític	19,0%
Els usuaris no poden connectar dispositius externs de memòria a l'equip de treball	No crític	18,9%
Existeix un control de tràfic entre la xarxa externa i la interna	No crític	16,7%
La contrasenya és robusta	No crític	10,7%