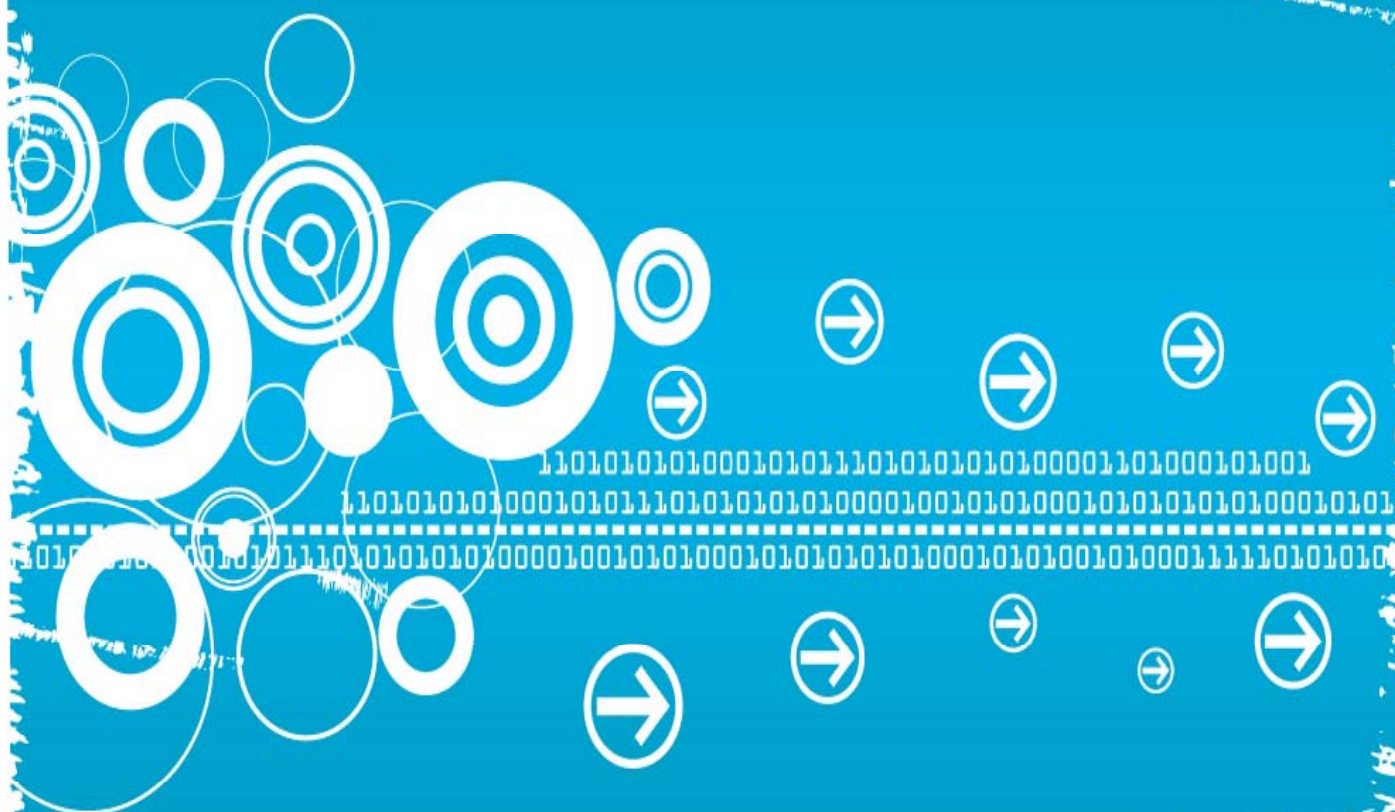


Guia de seguretat TIC



ÍNDEX

1.	Introducció	2
2.	Marc Normatiu i Legal.....	4
3.	Implantació d'un sistema de seguretat	6
4.	Eines de seguretat bàsiques	9
5.	Recomanacions de seguretat.....	15
6.	Tendències	16
7.	Cas pràctic	17
8.	Consells de seguretat	18
9.	Links relacionats	19
10.	Glossari	20

1. Introducció

La contínua transformació i la necessitat de canvi i millora en el sector TIC fan que molt sovint es deixi de banda la seguretat quan es alhora un dels punts mes importants i que pot afectar directament a la productivitat.

L'objectiu principal de la guia que presentem es doble. Per una part es pretén que les PIMEs i MICROPIMES realitzin un anàlisi intern de la seva situació actual vers la seguretat de la seva infraestructura TIC. Per altra banda es vol fer conèixer quins son els punts mes importants que es poden aplicar per minimitzar els riscos actuals i els que segurament aniran sorgint. La gravetat d'aquestes incidències pot arribar a ser important en cas de pèrdua de informació sensible o el robatori de dades per fer un us fraudulent i que poden derivar en problemes tant econòmics com legals. Tot i que pot semblar que el tant per cent de PIMEs afectades es baix, cal considerar que la majoria de incidències no es fan publiques degut a la publicitat negativa que poden ocasionar.

Els aspectes de la seguretat que cal tenir en compte son els següents:

Disponibilitat: Assegurar que les dades sempre son disponibles per els usuaris autoritzats, en el temps acordat.

Confidencialitat: La informació només pot ser accessible per els usuaris autoritzats segons la classificació adoptada.

Integritat: Cal garantir que la informació rebuda no es modifica i es exactament igual a la original que va generar l'emissor.

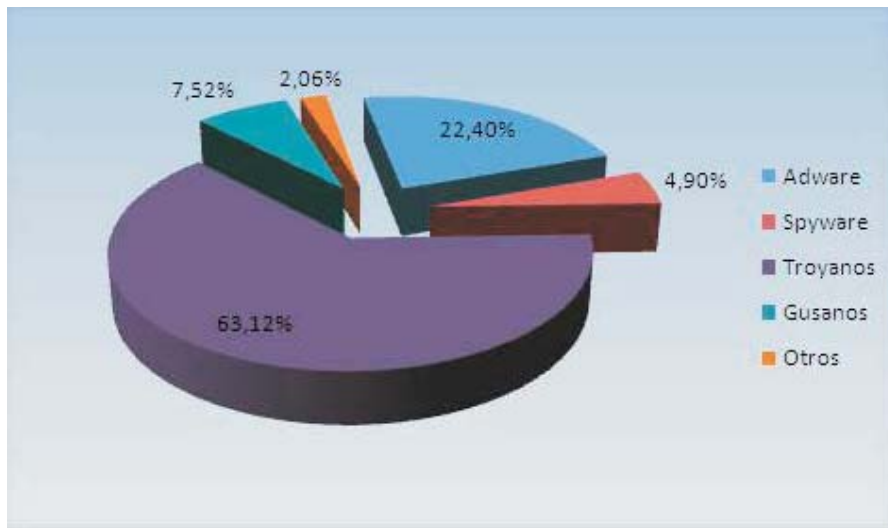
Autenticació: La persona que realitza una identificació electrònicament és qui diu ser realment.

Traçabilitat: Saber l'origen, històric de modificacions i accessos a la informació.

Un dels creixements mes elevats ha estat el nombre de casos detectats de malware (terme general adoptat per tot els programes que contenen codi nociu destinat a recollir informació o causar alguna incidència)

La globalització de les xarxes mitjançant Internet ha incidit mes que mai en aquest aspecte. De la mateixa manera que la connectivitat global ha permès ampliar la capacitat de negoci, també ha incrementat el nombre de riscos al que hem de fer front. En un principi Internet va estar concebuda per treball en entorns de confiança i els protocols establerts no eren segurs. Ha estat la incorporació de activitats econòmiques el que l'han fet objectiu de atacs i s'han evidenciat les mancances de seguretat que cal anar eliminant.

El següent gràfic mostra els diferents tipus de malware on veiem que el més comú es el grup format per els Troians (programa nociu amb aspecte de legítim destinat a la captura i control il·legal de dades):



Font: Informe Trimestral Pandalabs

A banda de les incidències provocades per agents externs, també cal tenir en compte els aspectes relacionats amb els procediments interns de seguretat com pot ser disposar de un pla de contingència i recuperació de desastres el més eficaç possible. No cal oblidar que molts dels atacs es produeixen des de dins de la pròpia empresa.

Tot i que el riscs estan creixent a un nivell molt alt no cal ser alarmistes i si es compleixen les normes essencials de protecció podem minimitzar les possibilitats de pèrdua o divulgació no autoritzada de dades.

En matèria de normatives, trobem que cap al any 2000 degut a la creixent demanda d'una regulació en aquest tema per part de les empreses va sorgir la especificació internacional ISO17799 on es presenten un conjunt de controls que inclouen una sèrie de bones pràctiques de seguretat a l'empresa. Actualment s'està desenvolupant la família de normes ISO27000 incorporant nous aspectes que ajuden a generar un bon SGSI (Sistema de Gestió de la Seguretat de la Informació). Tot i que no exposarem com obtenir aquesta certificació si que donarem una idea dels punts bàsics que componen aquesta norma i de quina manera poden ser útils per a la PIME.

Al final del document trobarem una secció d'enllaços que poden ser útils alhora de cercar recursos i un glossari amb els termes més específics de la seguretat informàtica.

2. Marc Normatiu i Legal

La manca de compliment normatiu en matèria de seguretat a la PIME pot portar a sancions cap a la empresa que moltes vegades es desconeixen. Per evitar-les cal conèixer i aplicar el contingut especialment per el que fa a les lleis següents:

- **LOPD:** Llei 15/1999, de 13 de Desembre, de tractament de dades de caràcter personal. Té per objecte garantir i protegir les dades personals dels clients, proveïdors, personal, etc.. així com les llibertats públiques i els drets fonamentals de les persones físiques, i especialment la seva intimitat i privacitat personal i familiar. Si es disposa de fitxers amb dades d'aquest tipus cal inscriure's al registre de la AGPD (Agencia Española de Protección de Datos) i seguir les recomanacions de seguretat.
- **LSSI:** Llei 34/2002, de 11 de Juliol, de Serveis de la Societat de la Informació i de Comerç Electrònic. S'aplica a les activitats realitzades per mitjans electrònics de caràcter comercial o amb finalitat econòmica.
- **LISI:** Llei 56/2007, de 28 de desembre, de Mesures d'Impuls de la Societat de la Informació. Aquesta llei introdueix un seguit d'innovacions normatives en matèria de facturació electrònica i de reforçament dels drets de les persones usuàries i es realitzen les modificacions necessàries en l'ordenament jurídic a fi de promoure l'impuls de la societat de la informació. Per exemple es considera la banda ampla com a servei universal i es dona un impuls a la signatura electrònica.

A banda cal realitzar auditories de seguretat i disposar de un document de seguretat (**Guia de Seguridad** que podrem trobar a la web de la AGPD).

La necessitat de disposar de sistemes fiables davant del creixement de les tecnologies a les empreses i per facilitar l'acompliment de la legislació vigent es recomanable seguir les diferents normatives que han anat sorgint a nivell internacional i que tendeixen a unificar-se en el estàndard de seguretat format per la sèrie ISO27000. Tot i que actualment esta en procés de desenvolupament es molt possible que en un futur sigui un requisit necessari per oferir unes garanties de servei, sobretot per aquelles empreses que realitzin transaccions comercials per Internet.

Dins d'aquest conjunt de normes fins ara s'han elaborat els següents documents:

- ISO27000: En fase de desenvolupament, contindrà els termes i definicions que es faran servir a tota la sèrie.

- ISO27001: Es la norma principal de la que permet certificar-se i conté els requisits del sistema de gestió de seguretat de la informació. Té el seu origen en la norma BS7799 i especifica les normes de disseny, implementació, manteniment i millora del SGSI, els seus processos i els controls d'aplicació.

- ISO27002: Es una guia de bones pràctiques que descriu els objectius de control recomanables en quant a seguretat.

- ISO27003: També en desenvolupament, ajudarà i facilitarà la implantació del SGSI marcant unes guies per a una correcta implementació.

En projecte s'inclouen la resta de normes que s'aniran afegint a mida que es finalitzi la seva definició:

- ISO27004: Definició de mètriques i indicadors per monitoritzar el grau de funcionament dels sistemes

- ISO27005: Gestió de riscos de la seguretat en la informació

- ISO27007: Guia de auditoria ISMS (Information Security Management)

- ISO27008: Auditoria de controls de seguretat

- ISO27011: Guia implementació de un ISMS per la indústria de telecomunicacions

- ISO27031: Especificació sobre continuïtat de negoci (Disponibilitat dels sistemes)

- ISO27032: Aspectes de ciberseguretat a Internet.

- ISO27033: Seguretat de xarxes informàtiques.

- ISO27034: Guies de seguretat a les aplicacions.

Si es pot disposar dels recursos per tirar endavant la certificació es una opció interessant ja que proporciona un increment del valor comercial i la millora de la imatge de la empresa.

AENOR es la associació que regula les normes en l'àmbit espanyol. Està previst que es realitzi l'adaptació de ISO27000 a UNE que substituirà la actual UNE 71502 (Gestió de la Seguretat de la Informació) publicada al 2004.

3. Implantació d'un sistema de seguretat

Es imprescindible partir de la base que per implantar les eines i procediments de seguretat, la direcció o gerència han pres aquest tema com un element estratègic de l'èxit de la empresa.

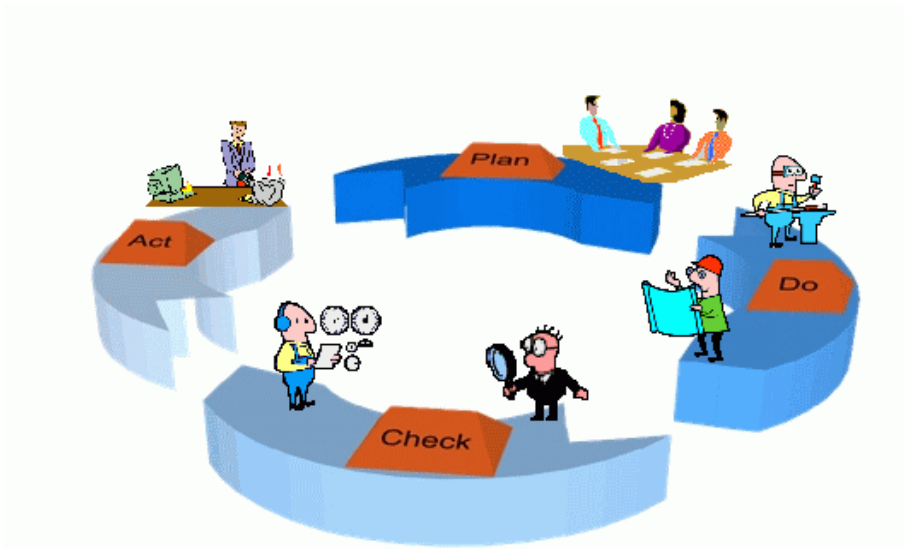
Per tal d'afrontar el procés de implantació ens podem decantar per contractar els serveis d'una consultoria o bé dedicar-hi recursos propis. En qualsevol cas tant la direcció com els empleats s'han d'implicar plenament en el procés donat que afecta a la operativa diària de la empresa. En el cas de les PIMES ens trobem que cada empresa té la seva manera de treballar per tant s'hi haurà de implicar molt més que una gran empresa que funciona de manera més estàndard. L'avantatge és que el volum de processos serà molt menor i facilitarà l'adopció de les mesures de seguretat.

Els beneficis de contractar un proveïdor especialitzat per generar la definició del pla de seguretat de la nostra empresa es basen en la delegació en mans expertes de la matèria amb el que estalviem el temps de dedicació i si es realitza correctament es garanteix la qualitat del procés. Els inconvenients els trobem en el cost del servei i el treball dedicat a triar un proveïdor que ofereixi garanties i amb el que tinguem un bon enteniment, cosa que no sempre es així.

Cal remarcar la importància de realitzar un esforç de dedicació de recursos humans donat que ha de ser completa i veure-ho com una inversió i no com una despesa. Per exemple la pèrdua o subtracció de dades poden causar un impacte econòmic molt més elevat que els que caldria haver-hi dedicat. Per tal d'assumir el creixement de la producció de les PIMES cal integrar els processos principals a les TIC i això produeix que una incidència greu en el sistema informàtic paralitzi la producció durant un temps determinat amb les pèrdues que pot ocasionar.

Seguint la filosofia definida per la norma ISO tractada a l'apartat anterior, per implantar un SGSI s'utilitza el cicle continu PDCA (Planificar, Realitzar, Comprovar, Actuar) tradicional en els sistemes de gestió de la qualitat que defineix d'una manera ordenada les fases a realitzar:





1. Plan: Anàlisi dels processos de la empresa identificant punts crítics i riscos. Un primer pas seria definir quins son els processos de treball de la empresa i quins elements TIC hi ha involucrats. Un cop definits cal classificar-los segons la seva importància i possibles amenaces als que estan sotmesos. D'aquesta manera podrem comprovar quins son els aspectes on hi hem de implantar mes millores o quins hem de reforçar mes. Un altre aspecte d'anàlisi es la detecció dels punts de entrada de dades, per exemple una connexió ADSL via WIFI.

2. Do: Instal·lació de la solució mes adequada en cada cas en funció de les necessitats detectades al pas 1. Per exemple si hem detectat que un procés important és l'enviament de correus electrònics a clients caldrà identificar el servidor de correu i protegir-lo amb una eina antivirus i antispam.

3. En aquesta línia ha de quedar molt clar que s'han configurat correctament les eines instal·lades i es van actualitzant per necessitats internes o perquè el proveïdor ha desenvolupat una millora necessària. Som nosaltres els responsables d'aplicar aquests canvis en la nostra infraestructura.

Check: Monitorització i avaluació dels resultats.

Un cop implementades les eines i processos requerits en cada cas, cal fer un seguiment de la seva efectivitat. Per exemple cal implementar un procediment de comprovació de còpies de seguretat. En aquest anàlisi comprovarem les variacions en la duració i quantitat de dades de la còpia i comprovarem que siguin conseqüents i que no hi ha cap error ni avís als logs del procés.

4. Act: Millora contínua dels processos. Un cop realitzat el procés caldrà tenir en compte que no es puntual sinó que caldrà anar-lo adaptant als canvis i afegint millores que aportin la experiència o la cerca de noves solucions. En el cas que tinguem un document on es detallin les normes

d'actuació en relació amb el intercanvi de informació amb tercers, caldrà actualitzar-lo en el cas que canviem un dels proveïdors que tenen accés a la nostra informació.

En aquest sentit cal seguir actualitzant-se mitjançant Internet, premsa o jornades de seguretat que es vagin realitzant i adaptant les noves tècniques que van sorgint. La formació i la conscienciació sobre el nostre sistema de seguretat cal fer-la arribar a tots els empleats de la empresa i cal fer un seguiment del seu compliment per part de tothom, orientant-ho com una ajuda cap a la feina i fent veure que no es tracta de posar simples impediments al treball diari.

Com a resum de les avantatges que pot aportar un bon SGSI destaquem:

- Facilitat de gestió i efectivitat del sistema de seguretat de l'empresa
- Disponibilitat de servei màxima
- Millora dels processos comercials per canals electrònics.
- Disposar d'una bona posició davant de auditories i l'entorn legal.

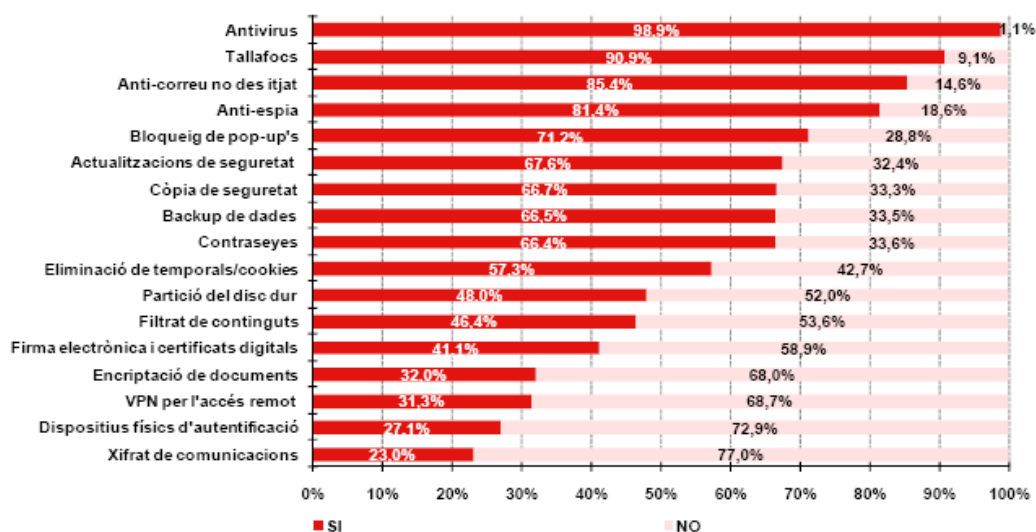
Millora de la imatge de la empresa davant de clients i proveïdors.



4. Eines de seguretat bàsiques

A continuació mostrem les eines bàsiques de seguretat que tota PIME hauria de tenir instal·lades i amb un control del seu funcionament. El nivell d'implantació i coneixement entre les PIMEs es divers tot i que podem dir que per el que fa a les eines de navegació a Internet es bastant alt (antivirus, antispam, tallafocs) no es així en altres mesures com el xifrat de les comunicacions, el control de accessos o els dispositius físics de autenticació.

El següent gràfic mostra el nivell de implantació de les mesures de seguretat:

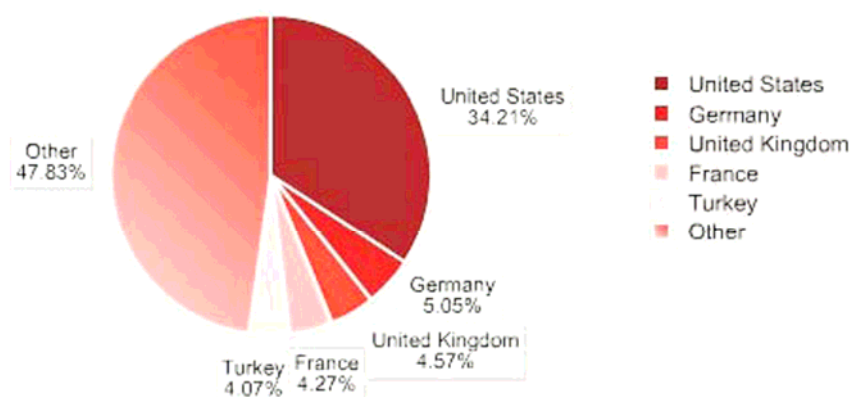


Opinions no contrastades

Font: INTECO

La seguretat total no existeix però si implementem les mesures adequades al nostre negoci podem assolir unes probabilitats molt petites de risc que ens permetin assegurar que disposem de un sistema segur.

El programari Antispam bloqueja el correu electrònic no desitjat, també anomenat SPAM o correu brossa. Normalment es correu publicitari però en determinats casos també poden incloure algun tipus de malware. Tot i que esta prohibit per llei realitzar aquests enviaments massius, la dificultat de identificar l'origen fa que actualment sigui un problema a tractar. Estats Units es el país que mes spam origina:



Font: Commtouch Software online Labs

Per la empresa els beneficis associats d'activar una eina d'eliminació de correu no desitjat son:

- Increment de la seguretat en el correu electrònic de la empresa
- Estalvi de temps i esforços en l'eliminació de SPAM (bloquejar, eliminar, activar, etc..)
- Minimització dels errors derivats de l'eliminació equívoca de correus electrònics
- Millora de la imatge de l'empresa

A nivell local cada aplicació s'haurà d'instal·lar en el corresponent gestor de correu determinat.

Tanmateix caldrà definir:

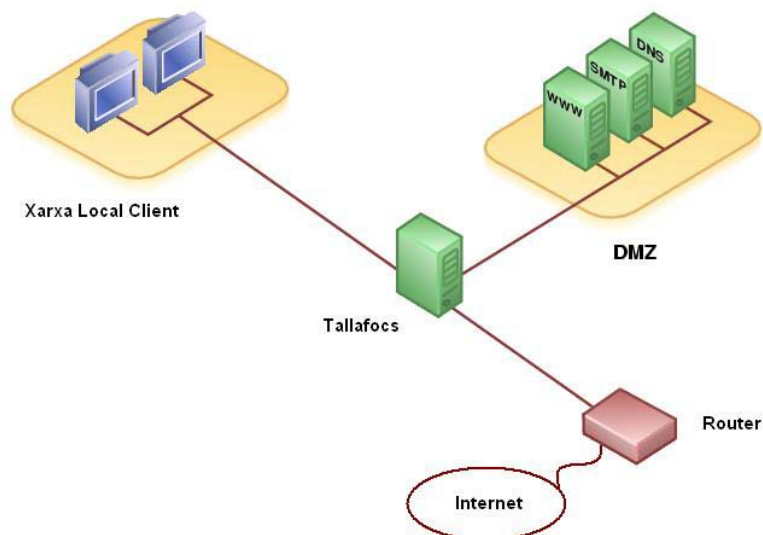
- Política d'entrada de correu
- Política d'eliminació del SPAM (automàtica, manual)
- Política de bloqueig de comptes o dominis sospitosos.

La externalització d'aquest servei ens pot estalviar el temps de gestió de eliminació de SPAM i el espai ocupat als servidors tot i que cal assegurar-se que no bloquegen correu desitjat.

Sistema de Tallafocs

Un bon sistema tallafocs (també anomenat Firewall) es imprescindible per protegir la nostra infraestructura TIC dels atacs externs. La xarxa es un dels punts més sensibles del sistema informàtic donat que es la responsable de comunicar les dades i també les amenaces. Si tenim connexió a Internet, ens permet bloquejar els intents de accés no autoritzat.

A nivell esquemàtic el tallafocs cal situar-lo entre la connexió a l'exterior i la nostra xarxa:



En el cas que disposem de equips que ofereixen serveis al exterior com per exemple un servidor de pàgines web, aleshores harem de situar-los en una zona anomenada DMZ (Zona Desmilitaritzada) o xarxa perimetral que permet rebre connexions de l'exterior però no té accés a la xarxa local interna del client.

La majoria de sistemes operatius i dispositius de router ja contenen aquesta aplicació i en casos on la seguretat no ha de ser molt alta ja van bé. Per exemple alguns només filtren el trànsit d'entrada i es recomanable també analitzar el de sortida.

Per la filosofia d'un tallafocs, a diferència dels antivirus que cal anar actualitzant, els tallafocs es configuren a mida que es necessita i ja no cal actualitzar-lo a excepció que el fabricant detecti alguna vulnerabilitat al cos del programa i desenvolupi algun pedaç.

Sistema de Antivirus i AntiSpyware

Aquesta es la mesura de seguretat més àmpliament implantada. Degut al efectes i la publicitat dels virus informàtics i altres programes maliciosos (Malware) han originat un ampli coneixement de les eines per anul·lar-los i gairebé totes les PIMEs disposen d'un software antivirus.

Segons la definició estricta de programes espia (o spyware) tot i no causar efectes destructius, recullen informació del equip infectat sense el seu consentiment. Existeixen programes específics per eliminar spyware tot i que els antivirus més recents ja incorporen la eliminació o bloqueig de programes espia.

Cal protegir tots els equips de la empresa i anar-los actualitzant amb les definicions de nous virus i les millores del programa. Aquesta tasca s'acostuma a realitzar automàticament ja que molts dels programes inclouen la actualització i distribució de noves versions automàtiques.

Sistema de Còpies de seguretat

Les còpies de seguretat són un element imprescindible en cas de pèrdua accidental de informació. El primer que cal decidir abans de fer les còpies de seguretat és la estratègia que volem seguir, analitzant quin és el propòsit i l'entorn que ha de cobrir la còpia de seguretat. Ha de cobrir una estació de treball o una xarxa corporativa?

L'estudi de la importància i freqüència de modificació de les dades ens marcarà la planificació (numero de còpies) i la retenció (temps que volem guardar les dades). Cal tenir en compte que per exemple hi ha dades que per temes legals cal guardar-les 5 anys, per tant ens hem d'assegurar de realitzar un dia l'any una còpia total amb aquesta retenció.

Es important procedimentar les còpies creant una fitxa per cada equip que calgui copiar indicant tots els detalls necessaris com pot ser la descripció i nom de l'equip, fitxers que cal copiar, planificació, retenció, etc..

Els tipus de còpies més realitzats en una PIME són els següents:

- Còpies diàries

- Es realitzen diàriament per salvaguardar aquella informació que canvia cada dia
- En molts casos aquestes còpies es queden dins el mateix entorn que les dades originals (no es desen en un entorn segur)
- Permeten la ràpida recuperació de dades en cas de incidències puntuals

- Còpies periòdiques

- Es realitzen setmanal o quinzenalment depenent de la quantitat d'informació que canvia cada dia.

- Normalment s'extreuen de l'entorn de la empresa per poder recuperar en cas de desastre a la ubicació original. Es important mantenir un registre amb les entrades, sortides i destí dels suports, així com la autorització de un responsable.
- Permeten la recuperació de dades en cas de fallades importants

- Còpies històriques

- Es recomana fer-les cada cop que fem tancaments comptables, de facturació, anuals, etc..
- Ens han de permetre mantenir un històric de les dades més importants de la empresa (comptabilitat, factures, projectes, etc..)

- Còpies de sistema

- Es realitzen per a aquells ordinadors que en cas de fallar no podem tenir aturats durant períodes llargs de temps
- Salvaguarden el funcionament d'un o més ordinadors o servidors però en cap cas emmagatzemen les dades de la empresa

Hi ha diversos dispositius físics contra els que podem fer les còpies de seguretat. La decisió vindrà donada segons factors determinants com pot ser la quantitat de dades a copiar, la velocitat o el cost de la solució.

El dispositiu més comú es la cinta magnètica. Les cintes ens permeten emmagatzemar grans quantitats de informació a un baix cost, aquest es un dels sistemes més usats, en contraposició de que es un dels sistemes que tenen un major cost de temps per recuperar la informació. Alguns exemples son les cintes DAT (Digital Audio Tape) amb capacitats de fins a 80 GB o be LTO (Linear Tape Open) que arriben fins a 800 GB en el cas de LTO-4.

Les còpies d'un sol ordinador o d'una estació de treball es poden fer de forma còmode utilitzant un DVD. La majoria d'estacions de treball d'avui dia permeten copiar la informació en suports DVD. Aquesta tecnologia es pot combinar amb d'altres per garantir un major nivell de còpies de seguretat.

Te una capacitat per a 4.7GB i fins a 9.4GB en discs de doble cara.

Les memòries i discs USB cada cop mes populars ens permeten enregistrar ràpidament cada cop més quantitat d'informació. Cal remarcar que la seva sensibilitat a l'entorn es major que altres sistemes.

Els serveis de còpies online estan cada cop mes extesos. Aporten avantatges com l'abaratiment de costos, disponibilitat immediata de les dades en qualsevol lloc amb accés a internet i la

seguretat creixent, tot i que cal assegurar-se que la empresa que proporciona el servei compleix les normes sobre seguretat.

Per grans quantitats de dades, la velocitat de les comunicacions poden ser un coll d'ampolla que impedeixin la productivitat d'aquesta opció.

Sistemes de xifrat de dades

Si en el estudi previ del nostre sistema d'informació s'han detectat dades confidencials o d'un alt nivell de seguretat, cal contemplar la possibilitat de xifrar les dades mitjançant eines criptogràfiques.

Una de les aplicacions mes comunes es el dels certificats digitals. Ens permet generar signatures digitals que després podrem fer servir per exemple per generar factures electròniques o per xifrar els enviaments de correu electrònic.

Amb la signatura digital o electrònica podem garantir la autenticitat del emissor o signant de un document així com la integritat del contingut signat.

Per sol·licitar un certificat digital cal dirigir-se a una entitat anomenada Autoritat de Certificació.

Podem consultar a la web del Ministerio de Industria, Turismo y Comercio el llistat oficial:

<http://www.mityc.es/DGDSI/Servicios/FirmaElectronica/Prestadores>



5. Recomanacions de seguretat

Amb la implantació d'un sistema de seguretat el que obtenim es una reducció del nivell de risc al que estem exposats. D'una manera esquemàtica podem resumir les següents bones pràctiques en matèria de seguretat:

Nivells	Riscos	Solucions
Xarxa de dades	Atacs per intrusió Robatori d'ample de banda Captura de dades en la transmissió	<ul style="list-style-type: none"> - Us de tallafoc en punts d'accés a Internet - Protegir les xarxes WIFI amb claus segures - Contemplar sistemes IDS/IPS (Sistema de Detecció/Prevenció de Intrusos) - Implementar VPN (Xarxa Privada Virtual) en cas de telefonia IP o accessos remots per xifrar les comunicacions. - Fer servir protocols segurs en transaccions comercials per xarxa.
Continguts	Infecció de fitxers (malware) Modificacions no autoritzades de pàgines web Robatori de informació Pèrdua de servei per incidència al programa Correu brossa Phising	<ul style="list-style-type: none"> - Us de Antivirus, Antispyware i Antispam - Filtrat de continguts web. - Definició de protocols de intercanvi i accés a les dades per part de tercers (subcontractacions, externalitzacions) - Creació de documents de seguretat, confidencialitat i secret i fer-lo signar a tots els empleats.
Dades físiques	Incendi o robatori dels servidors Eliminació per error de les dades Problema en les actualitzacions Incidències en el subministrament elèctric	<ul style="list-style-type: none"> - Definir política de còpies de seguretat - Sala CDP acondicionada amb seguretat perimetral i control d'accés. - Disseny professional del sistema elèctric i instal·lació de SAIs - Procediments i normes per al personal en contacte amb els sistemes de informació - Establir pla de continuïtat de negoci en cas de desastre - Implantar sistemes de alta disponibilitat

6. Tendències

L'accés cada cop més majoritari de les TIC a les empreses i la població en general fa que la innovació en el camp de la seguretat prengui una importància elevada. En aquest sentit s'estan desenvolupant sistemes amb una tecnologia complexa però fàcils de utilitzar i gestionar.

Per el que fa la seguretat física trobem els dispositius de seguretat biomètrica.

Es basen en la captura de dades físiques i de comportament de un individu per identificar la seva identitat. Els sistemes que ja podem veure instal·lats en algunes empreses son el reconeixement de les empremtes dactilars, el iris o la retina. La fiabilitat i facilitat de us del sistema son mes elevats que els sistemes tradicionals de tarja o numero PIN però també presenten inconvenients com el cost de instal·lació i certs problemes en casos de fals positiu o engany al sistema mitjançant reproduccions com podria ser un escaneig de empremtes.

Respecte a la seguretat lògica, podem trobar que en el camp de les xarxes, s'està avançant en les tecnologies cap als sistemes IDS / IPS (Sistemes de Detecció/Prevenió de Intrusions). Amb aquests programes poden detectar de manera intel·ligent els atacs i intents d'accés a la nostra xarxa. El funcionament es basa en l'anàlisi del trànsit de la xarxa i la cerca de patrons o comportaments sospitosos. Aquest component s'integra amb el tallafocs que representa la primera línia de defensa contra els atacs.

Finalment, comentar que en el camp de l'administració pot ser molt útil per a la PIME les eines UTM (Gestió unificada d'amenaces). Els sistemes ja contenen tots els elements necessaris de seguretat i son útils per poques quantitats de dades o per entorns on volem facilitar la gestió i administració donat que es realitza des de una única interfície.

Presentats habitualment en format hardware, a banda dels elements de seguretat també incorporen servidors web, correu, DNS i proxy.



7. Cas pràctic



SERVEIS ADMINISTRATIUS PERES, SLL es una gestoria on hi treballen 10 persones. Tots ells fan un ús intensiu del correu electrònic i d'Internet.

El volum de feina és important, però sobretot, en moments concrets de lliurament de impostos (IVA, impost de societats, rentes,...).

Per part de gerència es detecten els següents problemes i necessitats:

- Pèrdua de temps important amb correus que no són únicament de feina
- Baixada de la productivitat en més d'una ocasió per l'entrada de virus i d'altres atacs
- Voluntat de tenir control sobre l'ús d'Internet per finalitats no professionals
- Possibilitat de treball remot per alguns dels empleats

Es fa la corresponent auditoria per tal de detectar la situació real i poder dibuixar així el millor esquema per la solució indicada i es detecta el següent:

- No es disposa d'una solució antivirus actualitzada
- No hi ha control del spam i, tant el correu electrònic, com la navegació a Internet, es fa directament a través del router de l'operador sense cap tipus de protecció
- Cada treballador té la seva pròpia conta de correu i la política de protecció de dades és adequada a nivell del servidor de domini i les aplicacions de gestió

És així com es valora la possibilitat d'implementar les diferents solucions:

- Sonicwall TZ190, dispositiu Firewall que ens permet:
 - o Control de l'ús d'Internet i reportar-ne, per a cada usuari, les pàgines visitades. Es poden adoptar diferents polítiques de restricció en funció del què es detecti i és per això que es decideix posposar la definició de les restriccions en funció de l'anàlisi de tot un mes d'ús.
 - o Possibilitat d'accés remot a través del client VPN, podent establir les mateixes polítiques de seguretat que existeixen a l'oficina, limitant (si s'escau), la informació de què es pot disposar en remot en funció de cada usuari
 - o Protecció dels atacs exteriors a través del Router

COST TOTAL DE LA INVERSIÓ 750 €

- Sonicwall Email Security que ens permet:
 - o Filtrat i anàlisi del correu electrònic de sortida i entrada
 - o Actualització automàtica del motor antivirus per a la protecció de les contes de tots els usuaris de forma automatitzada i amb una gestió simplificada

COST TOTAL DE LA INVERSIÓ 2.000 €

8. Consells de seguretat

Es recomana mantenir les aplicacions i el sistema operatiu a la última versió disponible i es imprescindible anar aplicant els pedaços de seguretat tant aviat com surtin publicats. Si es possible primer provar-ho en un entorn similar al de producció.

No obrir correus de fonts no confiables i no obrir adjunts no verificats encara que procedeixin de fonts conegudes.

No respondre als correus d'enviaments massius tipus cadena de mail ja que la major part saturen els servidors. En cas que calgui enviar-lo posar les adreces en el cap de copia oculta ja que moltes vegades serveixen per capturar adreces de mail a les que fer-li spam.

Mai s'ha de comunicar a ningú les contrasenyes d'accés de cap tipus. No hi ha cap raó excepte que vulguin accedir a les nostres dades per que ens les demanin encara que siguin els administradors o l'entitat on s'accedeix.

Compte amb la instal·lació de programes per compartir fitxers tipus peer-to-peer. Son potencialment perillosos i cal assegurar-se si cal instal·lar-lo en equips productius.

Cal fer servir sempre sistemes d'alimentació ininterrompuda (SAIs) per tal de protegir-se davant de talls, microtalls i pujades o pics de tensió al subministrament de corrent elèctric que alimenta els sistemes informàtics. En aquest sentit podem evitar que els processos que s'executen en el moment de un tall s'aturin de cop i es produeixi una possible pèrdua de dades o fins i tot la avaria física de l'equip, a banda del temps que es perd recuperant el servei.

No instal·lar més de un programa de seguretat del mateix tipus ja que es detecten entre ells i poden inutilitzar el servei.

En les transaccions comercials per Internet cal fer servir sempre protocols segurs i si es disposa de algun sistema de claus i certificats digitals incrementarem el nivell de privacitat.

Es molt recomanable no treballar amb les comptes de usuaris amb privilegis d'administrador (windows) o root (unix/linux). Cal crear usuaris amb els permisos mínims necessaris per el treball diari.

Quan no estem davant de l'ordinador sempre deixar la sessió bloquejada amb contrasenya segura i deixar l'escriptori net de papers que puguin incloure dades personals o confidencials.

9. Links relacionats

Informació general:

www.agpd.es → Agencia de Protección de Datos

www.inteco.es/seguridad → INTECO - Institut Nacional de Tecnologies de la Comunicació

alerta-antivirus.inteco.es → Centro de Alerta Temprana sobre virus y seguridad

www.hispasec.com → Seguretat i tecnologia

www.iso27000.es → Estàndard Sistema de Gestió de Seguretat de la Informació

www.enciclopediavirus.com → Informació sobre virus

seguridad.internautas.org → Associació internautes

www.sans.org → SANS Institute - Network, Security, Computer, Audit Information & Training

Signatura digital:

www.cecot.es/rea → Registre empreses acreditades de Catalunya - Cecot

www.anf.es → ANF Autoridad de Certificación

www.catcert.net → CATCert - Agència Catalana de Certificació

www.facturae.es → Facture electrònica – Ministeri de Economia i Hisenda

www.seres.es → Proveïdor factura electrònica

Proveïdors tecnologia:

www.symantec.com -> Antivirus i còpies de seguretat comercial.

www.spamfighter.com -> Antispam gratuït

www.grisoft.com -> Antivirus gratuït

www.zonealarm.com -> Tallafocs Shareware

esp.sophos.com -> programes antivirus i anti-spam per a empreses

www.solunix.es -> Serveis empresarials, inclou seguretat

www.tb-security.com -> Consultora seguretat

www.gestinet.com -> Informàtica i comunicació

10. Glossari

Autenticació: Procés mitjançant el qual es comprova la identitat de un usuari

Autorització: Dret atorgat a un individu autenticat o procés per a utilitzar el sistema d'informació i la informació que conté.

Certificat digital: Sistema acreditatiu que conté informació de un usuari o servidor per a la verificació de la seva identitat en el sistema de informació.

Cracker: Persona que s'introdueix il·legalment en un equip informàtic amb intencions de causar algun tipus de incidència o acte malintencionat.

Encriptació: Procés mitjançant el qual la informació es codificada per evitar l'accés a usuaris no autoritzats.

Malware: Programa informàtic que té per objectiu infiltrar-se en un equip sense el coneixement del usuari o administrador amb finalitats malicioses.

Troia: Es un tipus de malware que permet l'accés no autoritzat als nostres equips amb la finalitat d'obtenir informació privilegiada o be pendre el control de la màquina atacada.

Pedaç: En l'argot informàtic, un pedaç és una secció de codi que s'inclou a un programa amb l'objectiu de corregir algun problema detectat posteriorment o afegir-li funcionalitats.

Phishing: Estafa basada en enginyeria social on es demanen els codis secrets via correu electrònic simulant ser la entitat original o una oficial. Ni els bancs ni cap administrador de xarxa demanen mai les claus.

Spam: També anomenat correu brossa, és tot aquell correu electrònic no desitjat enviat de manera indiscriminada. Habitualment tenen objectius publicitaris tot i que també poden servir per difondre algun tipus de malware.

Spyware: Es un tipus de malware dedicat a recopilar informació privada d'un equip informàtic sense el consentiment del usuari. Habitualment tenen objectius publicitaris tot i que poden recopilar informació per realitzar un estil d'espionatge.

Zombie: Ordinador infectat sense que el propietari en sigui conscient i utilitzat per realitzar altres atacs ocultant la identitat original del delinqüent.

