TALLER 2

GESTIÓ DE LA SEGURETAT I NORMES ISO 27000

Curs: PQTM 19. Tècnic/a en Ciberseguretat

Ivan Ricart Borges iricartb@uoc.edu

ÍNDEX

1. Descripció de la ISO 27000 i 22301.....3
2. Descripció de la fitxa 22301 a la web de la ISO.....3
3. Descripció de la fitxa 27002 a la web de la ISO.....3
4. Descripció de dos dels dominis de la ISO 27002.....4
5. Fonts d'informació.....5

1. Descriviu, utilitzant les vostres paraules i amb una extensió d'entre 10 i 12 línies, en què consisteixen la ISO 27000 i la ISO 22301.

La ISO 27000 forma part d'una família en creixement d'estàndards, tots ells, relacionats amb els Sistemes de Gestió de la Seguretat de la Informació (SGSI), podríem dir que es el punt de partida d'aquest conjunt i que proporciona una introducció, una visió general de les normes, una breu descripció del procès (PDCA) i finalment un vocabulari o glossari de termes. La seva principal finalitat és ajudar a les organitzacions a implementar i operar un Sistema de Gestió de la Seguretat de la Informació.

La ISO 22301 és una norma auditable i pionera, dissenyada per a que el negoci continuï, encara que es produeixin circumstàncies desafiants i inesperades. Proporciona una base per entendre, desenvolupar, implantar i gestionar la continuïtat del negoci dintre de la empresa i donar confiança sobre les parts afectades proporcionant mecanismes d'actuació un cop s'ha materialitzat el dany, es a dir, gracies a aquesta norma, la organització estarà preparada per respondre de forma adequada i així reduir dràsticament el dany potencial del incident.

2. Descriviu en què consisteix la ISO 22301 i expliqueu de forma resumida el que n'explica la fitxa a la web de la ISO.

En la web de la ISO, la informació de la fitxa està estructurada de tal manera, on primerament es fa una breu descripció de la norma, posteriorment s'especifica una sèrie d'informació genèrica, com per exemple, l'estat actual (Publicat), la data de publicació (Maig 2012), la versió de correcció (Juny 2012), el número d'edició (1), el número de pàgines (24), el comitè tècnic encarregat (ISO/TC 292), número de Classificació Internacional del Estàndard (ICS 03.100.01 i ICS 03.100.70), finalment permet la seva compra proporcionant diferents tipus de formats (PDF + EPUB, PAPER, PDF). Es important recordar que la seu principal de la ISO està ubicada a Suïssa, degut això, la pàgina oficial mostra la informació monetària amb francs Suïssos.

3. Descriviu en què consisteix la ISO 27002 i expliqueu de forma resumida el que n'explica la fitxa a la web de la ISO.

La ISO 27002 és la norma de la sèrie 27000 que es considera com la guia de bones pràctiques en la gestió de la seguretat de la informació. La seguretat de la informació es defineix en el estàndard com la preservació de la confidencialitat, integritat i disponibilitat. La norma estableix la importància de l'anàlisi de riscos com a punt d'inici del procés i presenta catorze dominis de control indispensables per a fer una gestió integral, que van des de qüestions administratives, fins a aspectes de recursos humans.

En la web de la ISO, de forma anàloga al punt anterior, la informació de la fitxa està estructurada de la mateixa manera, primerament es fa una breu descripció de la norma i posteriorment s'especifica la informació genèrica del estàndard, es a dir, l'estat actual (Publicat), la data de publicació (Octubre 2013), el número d'edició (2), el número de pàgines (80), el comitè tècnic encarregat (ISO/IEC JTC 1/SC 27), número de Classificació Internacional del Estàndard (ICS 35.030), finalment permet la seva compra proporcionant diferents tipus de formats (PDF + COLOR & PDF + EPUB, PDF + EPUB, PDF + EPUB + REDLINE, PAPER).

4. Escolliu dos dels dominis d'aquesta ISO i feu-ne una descripció a partir del que trobareu als materials ("Implantació d'un sistema de gestió de la seguretat de la informació").

La organització de la seguretat de la informació és un dels catorze dominis especificats en la ISO anterior, ens indica que es necessari establir una estructura organitzativa i especificar el funcionament d'aquesta, tant dintre, com fora de la organització. S'han d'especificar els rols i les responsabilitats en cada cas, segregar les tasques, establir polítiques de seguretat de la informació en la gestió de projectes, etc.

Dintre d'aquest domini també podem incloure els controls relatius a la política de dispositius mòbils i el teletreball, sempre que sigui aplicable a la naturalesa de l'empresa.

La seguretat física i de l'entorn és també un domini clarament especificat en la ISO anterior, ens indica que es necessari protegir la informació i els equips d'accessos físics indeguts i de danys de qualsevol tipus, per tant, s'han d'adoptar mesures per controlar l'accés físic a edificis i sales, i establir, si cal, àrees segures amb controls específics de seguretat perimetral, protecció davant amenaces ambientals, continuïtat del subministrament elèctric, etc.

5. Fonts d'informació.

Recursos

Implantació d'un sistema de gestió de la seguretat de la informació [PDF].

ISO

Pàgina oficial - Informació genèrica de la ISO.

https://www.iso.org

ISO 22301

Descripció de la ISO 22301.

https://en.wikipedia.org/wiki/ISO_22301

Descripció del pla de continuïtat de negoci.

https://en.wikipedia.org/wiki/Business_continuity_planning

ISO 27000

Descripció de la ISO 27000.

https://en.wikipedia.org/wiki/ISO/IEC_27000

Descripció de la sèrie ISO 27000.

https://en.wikipedia.org/wiki/ISO/IEC_27000-series

ISO 27002

Descripció de la ISO 27002.

https://en.wikipedia.org/wiki/ISO/IEC_27002