ANNEX A.P

Informe d'auditoria de compliment

Anàlisi del compliment de la norma ISO/IEC 27001:2013

Autor: *Francesc Lucio Subirachs*

Empresa auditada: *Empresa XXXXX coop.*

Any realització: *2016*

Àrea a auditar: *Sistema Gestor Seguretat Informació*

Ìndex

1. Informació general

1.1 Introducció

L'empresa XXXX, que actua en el sector de la llibreria i material electrònic per a proveir escoles, particulars i empreses en el territori Espanyol, mitjançant canals electrònics i punts de venta i distribució vol revisar el grau de compliment del seu Sistema Gestor de la Seguretat de la Informació en línia amb la norma certificable ISO/IEC 27001:2013 i el seu codi de bones pràctiques ISO/IEC 27002:2013.

1.2 Objectiu

L'objectiu general d'aquesta auditoria que s'ha realitzat és el de identificar, avaluar i verificar el grau de compliment en les mesures de seguretat, prevenció, organització i planificació de l'empresa XXXX que descriu la norma esmentada.

1.3 Abast

L'auditoria es cenyeix a la revisió dels controls establerts per la norma ISO descrita i el grau de compliment que l'empresa XXXX ha decidit assolir, en els seus objectius i consideracions inicials. Per a aconseguir-ho l'empresa voldrà verificar que els projectes que s'han proposat per a la millora d'aquest compliment i correcta implantació i millora del SGSI (sistema gestor de la seguretat de la informació) han suposat (o no) un benefici substancial o considerable per a poder assegurar la seva continuïtat de negoci, financer, transaccional, social i comercial.

1.4 Equip auditor

L'equip auditor esta compost únicament per un auditor en cap, encarregat de dirigir, supervisar, realitzar les proves, mesures, conclusions, presentar i contactar amb els responsables de l'empresa per a poder executar i realitzar el seguiment del procés d'auditoria.

Nota: Per la dimensió de l'empresa no s'ha decidit incloure més auditors.

1.5 Interlocutors

En representació de l'empresa els membres del comitè de seguretat, on hi consta un representat de cadascuna de les següents àrees descrites: Recursos Humans, Administració, Vendes i Marketing, Serveis informàtics, Assessoria Jurídica, Distribució, emmagatzemament i relació amb proveïdors i Gestió de tendes; aquests són els encarregats de contactar amb el responsable de l'equip, sent aquests qui seran comunicats dels resultats, eventualitats i sent els mateixos qui informarà de tota modificació, desviació o el que es consideri oportú a l'equip auditor, subministrant-li la documentació i els accessos pactats per aquest comitè.

2. Execució de l'auditoria

2.1 Ubicació de l'auditoria

L'auditoria tindrà lloc en les instal·lacions següents:

- Serveis centrals de l'empesa, situades al carrer YYYYYY número NN a Barcelona, per a la revisió de la documentació, política, contractes i mesures de seguretat i instal·lacions d'aquest edifici, vehicles comercials i perímetres.
- Serveis logístics i magatzem de l'empresa, situat al carrer YYYYY del polígon industrial de la ciutat de CCCCC en el número NN, per a la revisió d'aquestes instal·lacions i la flota de vehicles associats en aquestes instal·lacions.
- Tenda situada al carrer YYYYY número NN de Barcelona.

2.2 Documentació revisada

La documentació requerida per a la realització de les proves, revisió i anàlisi del SGSI per a la realització de l'auditoria ha estat la següent:

- Contractes de proveïdors i serveis a tercers
- Pòlisses d'assegurança
- Contractes de vigilància i alarma
- Protocols i contractes de proveïdors de material o serveis distribució/virtuals
- Contractes d'altres serveis
- Contractes de locals i flota de vehicles
- Contractes de manteniment i serveis digitals
- Contractes de servidors i subministres
- Política de seguretat
- Estatuts i protocols de seguretat
- Normativa i organització de l'empresa
- Documentació
- Actes del comitè de seguretat

2.3 Tasques realitzades

Per a la realització d'aquesta auditoria s'han realitzat les següents tasques:

- Anàlisi inicial de la documentació i situació de l'empresa XXXXX.
- Establiment de la base documental per a l'auditoria interna de la seguretat.
- Identificació i valoració dels principals actius de l'empresa.
- Anàlisi de riscos, vulnerabilitats i amenaces de l'empresa i mesurament de l'impacte.
- Proposta i anàlisi de projectes de millora del grau de compliment inicial de la norma.
- Revisió de l'estat de compliment dels controls de la norma ISO/IEC 27001 segons el codi de bones pràctiques ISO/IEC 27002:2013 per al sistema avaluat després de la revisió i implantació dels projectes de millora i mitigació de riscos del SGSI.
- Presentació i elaboració de documentació amb els resultats dels procediments citats.

3. Presentació de resultats

3.1 Compliment de la norma

Es persegueix assolir els següent objectius, partint de la consideració que per a la realització de les conclusions i presa de decisions en base als resultats d'aquest Annex, es parteix de la coneixença de que la entitat pretén assolir un nivell de maduresa de, com a mínim, el 70%, tenint en compte que es parteix d'un compliment o aplicació inicial dels controls del 44% (definit en l'annex A.E).

- Obtenir una mesura del nivell de compliment dels objectius definits per la norma ISO/IEC 27002:2013 per a l'empresa proposada un cop aplicats els processos de control, millora i prevenció de riscos.
- Comparar el grau de compliment dels controls de la norma en els estats actuals (reals un cop aplicats els projectes) i esperats (esperats al definir els projectes).
- Mostrar una relació visual de l'estat de la maduresa del SGSI a partir d'un CMM

Grau de compliment dels controls

- En l'*annex, A.E - ítems posteriors a projectes,* s'especifiquen els graus de compliment dels controls i ítems definits per la norma un cop aplicats els projectes de millora i abans de fer-ho. A continuació es mostren únicament els controls i el seu percentatge de compliment actual.

Controls	Actual	Inicial	Esperat
5.POLÍTICA DE SEGURIDAD.	**100,00%**	30,00%	100,00%
6-ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	**88,90%**	46,07%	100,00%
7.GESTIÓN DE ACTIVOS.	**83,33%**	72,50%	100,00%
8.SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**43,33%**	36,11%	100,00%
9.SEGURIDAD FÍSICA Y DEL ENTORNO.	**80,60%**	53,81%	100,00%
10.GESTIÓN DE COMUNICACIONES Y OPERACIONES.	**87,36%**	66,88%	100,00%
11.CONTROL DE ACCESO.	**82,75%**	61,11%	100,00%
12.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	**55,36%**	20,33%	100,00%
13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**96,67%**	25,00%	100,00%
14.GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**100,00%**	23,00%	100,00%
15.CUMPLIMIENTO.	**100,00%**	0,00%	100,00%

- La següent taula mostra els resultats de maduresa segons els criteris definits en el CMM, en relació al valor percentual dels controls:

ESTAT PER NIVELLS DE MADURESA	
inexistent	1
adhoc	22
reproduible	53
definit	25
gestionat	20
optimitzat	41

Resultats

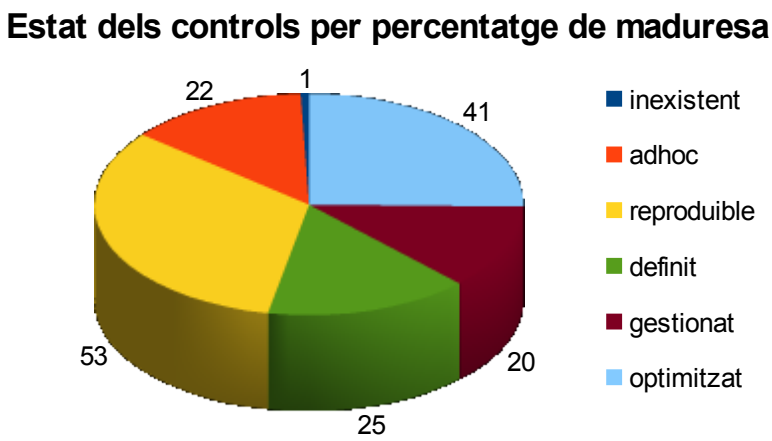
- El nivell de maduresa del sistema en base als controls exposats en el punt anterior és del 83% (83,48%); situant així el sistema i el resultat d'aplicar els projectes de millora de la seguretat com a mesures efectives i suficients per a suposar un increment de l'estat de seguretat i així complir l'objectiu de compliment proposat per l'empresa.

Estat de maduresa	83,48%

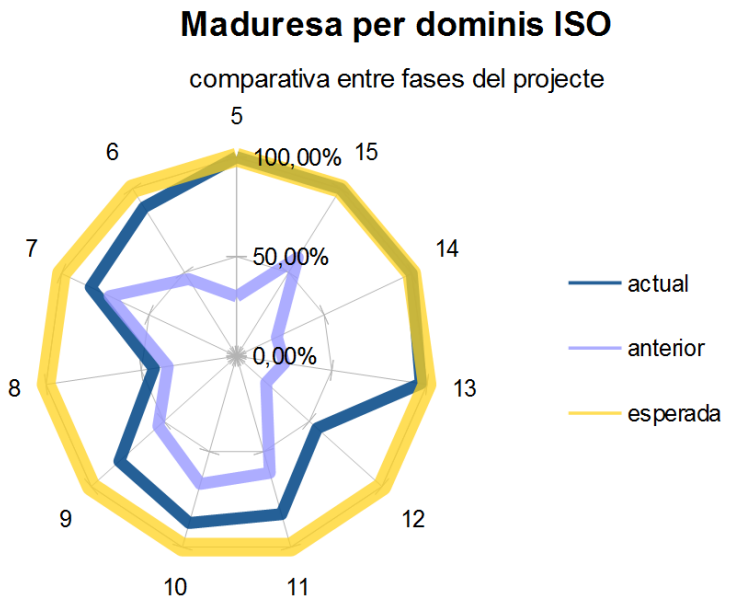
- El percentatge que cada nivell representa en el nostre sistema és el següent:

inexistent	1%
adhoc	14%
reproduible	33%
definit	15%
gestionat	12%
optimitzat	25%

- Els resultats obtinguts per a cada nivell de maduresa són els següents:



- En el següent diagrama de radar es pot observar la comparativa entre els nivells obtinguts, els esperats per l'organització i els inicials de forma conjunta.



3.2 No conformitats

Amb aquesta auditoria s'han detectat les següents no conformitats, d'acord amb el grau de compliment de la norma per als següents controls:

8. **Seguretat de recursos humans:** No conformitat de caràcter moderat

   Només s'han implementat i planificat millores en el requisit 8.2, amb la conscienciació i formació del personal, sense veure's incrementat ni planificat un pla de millora per a les fases prèvies i posteriors al contracte de treball a l'empresa.

8.SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**43,33%**
8.1 Antes del empleo.	**30,00%**
8.1.1 Funciones y responsabilidades.	**40,00%**
8.1.2 Investigación de antecedentes.	**20,00%**
8.1.3 Términos y condiciones de contratación.	**30,00%**
8.2 Durante el empleo.	**86,67%**
8.2.1 Responsabilidades de la Dirección.	**90,00%**
8.2.2 Concienciación, formación y capacitación en seg. de la inform	**100,00%**
8.2.3 Proceso disciplinario.	**70,00%**
8.3 Cese del empleo o cambio de puesto de trabajo.	**13,33%**
8.3.1 Responsabilidad del cese o cambio.	**10,00%**
8.3.2 Devolución de activos.	**10,00%**
8.3.3 Retirada de los derechos de acceso.	**20,00%**

12. **Adquisició, desenvolupament i manteniment de sistemes d'informació:** No conformitat de caràcter greu.

12.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**55,36%**
12.1 Requisitos de seguridad de los sistemas de información.	**100,00%**
12.2 Tratamiento correcto de las aplicaciones.	**57,50%**
12.3 Controles criptográficos.	**0,00%**
12.4 Seguridad de los archivos de sistema.	**46,67%**
12.5 Seguridad en los procesos de desarrollo y soporte.	**38,00%**
12.6 Gestión de la vulnerabilidad técnica.	**90,00%**

S'han implementat mesures de seguretat per als sistemes d'informació i el tractament de les aplicacions però no s'ha planificat millores per a xifrar la informació o mitigar vulnerabilitats i riscos de les fases de desenvolupament i suport dels sistemes informàtics.

4. Conclusions

Podem concloure que, partint dels objectius de l'empresa per aquest SGSI i la consideració inicial de compliment de la norma, s'ha assolit de forma genèrica el grau de compliment esperat, millorant així l'eficiència o efectivitat davant de potencials contingències i amenaces que puguin afectar al dia a dia de l'empresa, podent afectar la confiança, benefici o imatge del negoci. A més, s'ha desenvolupat un bloc documental per a totes les fases del projecte amb l'anàlisi detallat dels riscos als que ha de fer front l'empresa i dels projectes que han de millorar-ne la seguretat.

Com a millores o possibles punts a tenir en compte per a futures implementacions, es considerarà oportú i aconsellable que es realitzin auditories anuals sobre el sistema per a revisar que aquest esta actualitzat, adaptat i proporcionat a les amenaces, tecnologies i legislacions noves que puguin sorgir en un futur. A més, seria recomanable iniciar un pla exclusiu per a millorar el compliment dels punts que han generat no conformitats.