Resum executiu

Nom del projecte:	Projecte Final de Postgrau en Seguretat en serveis i aplicacions (PGAS)
Integrants del projecte:	Francesc Lucio Subirachs

Plantejament del projecte

Avaluar, millorar i definir plans per a la millora i el manteniment de la seguretat en una empresa en un entorn d'aplicació real, aplicant els estàndards internacionalment reconeguts ISO/IEX 27001 i 27002:2013 sobre el Sistema Gestor de la Seguretat de la Informació de l'empresa.

Justificació del projecte

Aplicar els coneixements adquirits al llarg de l'ensenyament de postgrau aplicats a un àmbit practic-real, mitjançant l'anàlisi i millora del SGSI d'una empresa basada en una organització real.

Objectiu

Establir les bases per a la realització del Pla director d'una empresa i la implementació d'un SGSI alineat amb els estàndards ISO internacionals i certificables per a la seva posada en marxa per a augmentar el nivell de seguretat de l'empresa i el seu impacte reputacional en tots els àmbits.

Desenvolupar, definir i identificar els riscos, vulnerabilitats i plans de millora de l'empresa i el seu SGSI.

Abast del projecte

El projecte es centra en l'estudi de l'estat de la seguretat de l'empresa en l'àmbit de l'anàlisi de riscos del SGSI descrit per la norma ISO/IEC 27001 i la definició de projectes per aconseguir elevar el nivell de compliment de la norma, perseguint en tot moment arribar als objectius i al llindar de compliment que estableix l'empresa en les assumpcions inicials del projecte.

Activitats rellevants del projecte

Per a la realització del projecte s'han dut a terme les següents fases, cadascuna de les quals es correspon a un anàlisi concret del SGSI:

1. Fase 1: Contextualització, objectius i anàlisi diferencial.
   - Introducció del projecte, definició d'objectius, anàlisi de la norma i descripció de l'empresa a analitzar.
2. Fase 2: Sistema de Gestió documental.

   Elaboració de la política de seguretat, declaració d'aplicabilitat i documentació del SGSI.
3. Fase 3: Anàlisi de riscos.

   Elaboració d'una metodologia d'anàlisi de riscos.
4. Fase 4: Proposta de projectes.

   Avaluació de projectes que ha de duu a terme l'organització per alinear-se amb els objectius plantejats inicialment.
5. Fase 5: Auditoria de compliment de la ISO/IEC 27002:2013

   Avaluació de controls, maduresa i nivell de compliment.
6. Fase 6: Presentació de resultats i entrega d'informes

   Consolidació dels resultats, realització d'informes i presentació executiva a direcció.

Resultat aconseguit

S'ha obtingut una valoració del compliment de la norma del nostre SGSI de l'empresa seleccionada, així com una valoració numèrica i mesurable del grau de protecció, valoració i d'exposició a amenaces dels actius més importants per a l'empresa.

Conclusions

S'ha determinat per a cada punt de l'anàlisi de riscos definit per la norma les valoracions i resultats del nostre SGSI.

S'han pogut proposar projectes de millora de la seguretat en els àmbits de mitigació de riscos ambientals i industrials, no intencionats i atacs intencionats, proposant tasques de revisió, actualització i compliment normatiu de la documentació i polítiques referides en cada cas, la revisió dels proveïdors i tercers (tals com asseguradores, seguretat, etc), la revisió de controls físics i lògics d'accés i la conscienciació del personal com un dels pilars per a prevenir moltes situacions que puguin afectar a la seguretat de la informació, dels propis treballadors, els actius o inclús la reputació de l'empresa.

Suggerències

Per a que aquest projecte, anàlisi i aplicació del SGSI, s'hauria de mantenir una planificació iterativa de millora i avaluació del mateix, fent les actualitzacions i revisions que la direcció o auditors externs creguin oportuna per adaptar-se a nous riscos, vulnerabilitats, actius o situacions que no s'hagin contemplat, ja que la clau d'un SGSI es la seva continua evolució i perfeccionament, així com la seva posada a revisió d'ulls experts per a auditar-lo.

Beneficiaris del projecte

El principal beneficiari de l'aplicació real d'un projecte d'aquest estil es l'empresa que s'avalua, ja que un procés de revisió, certificació i estandardització del SGSI beneficia tant a l'empresa, coma la seva reputació de cara als seus accionistes, inversors, clients, usuaris i proveïdors.