ATL
Ens d'Abastament
d'Aigua Ter-Llobregat

Codi del procés selectiu: ATL027-22TRE
Lloc de treball: Responsable de seguretat de la informació

Solucionari Test de coneixements prova teòrica del temari específic

Pregunta	A	B	C	D
1		X		
2	X			
3		X		
4				X
5	X			
6		X		
7			X	
8				X
9			X	
10		X		
11			X	
12			X	
13			X	
14				X
15			X	
16		X		
17		X		
18		X		
19	X			
20			X	
21				X
22			X	
23			X	

SOLUCIONARI PART PRÀCTICA

1. CAS PRÀCTIC : Proposta de solució a una empresa de distribució d'aigua

Multinacional del sector "utilities" està en fase d'expansió i evolució tecnológica. Presta serveis de potabilització i clavagueramen d'aigua en 10 paisos i 3 continents (Europa, Sudamérica i Africa). A España está implantada a 12 municipis i te 2 millions de clients. El seu creixement a estat mitjantçant adquisicions d'empreses mes petites locals.

En l'actualitat els clients exigeixen una millor experiència en interactuar amb aquesta empresa. La situació actual ha portat la junta a contractar un director executiu de tecnologia digital (CDO). El CDO treballa amb màrqueting i vendes per impulsar una transformació digital que potenciarà les experiències millorades. A més, diverses unitats de negoci van contractar recentment científics de dades per a les granges de dades i per millorar moltes de les experiències manuals mitjançant l'aprenentatge i la predicció. TI dóna suport a aquests esforços en la mesura del possible. No obstant això, s'estan duent a terme activitats de "TI a l'ombra" que queden fora dels controls de governança i seguretat necessaris.

L'organització de TI també s'enfronta als seus propis reptes. Finances està planejant reduccions contínues en el pressupost de TI durant els pròxims cinc anys, la qual cosa portarà a algunes retallades de despeses necessàries a partir d'aquest any. Per contra, els requisits de RGPD i altres requisits de govern de dades estan obligant TI a invertir en recursos que garanteixin la protecció de les dades. Dos dels centres de dades existents estan endarrerits en l' actualització de maquinari, la qual cosa causa més problemes amb la satisfacció dels empleats i els clients. Tres centres de dades més requereixen actualitzacions de maquinari durant l' execució del pla quinquennal. El CFO està pressionant el CIO perquè consideri el núvol com una alternativa per a aquests centres de dades, per tal d'alliberar despeses de capital. Veient la situació, el CIO demana la contractació d'un CISO que faciliti la implantació de les mesures de seguretat pertinents.

El CIO té idees innovadores que podrien ajudar l'empresa, però ell i els seus equips es limiten a apagar focs i controlar costos. En un dinar amb el CDO i un dels responsables de la unitat de negocis, la conversa sobre la migració al núvol va generar l'interès dels companys del CIO. Reben la grata notícia de l'aprovació per part de CEO de la contractació del CISO. L' objectiu dels tres responsables és recolzar-se mútuament en l' ús del núvol per assolir els seus objectius de negoci, i han començat les fases d' exploració i planejament de l' adopció del núvol.

Característiques empresarial

L' empresa té el següent perfil de negoci:

- Les vendes i operacions abasten diverses àrees geogràfiques.
- El negoci ha crescut mitjançant adquisicions i opera en tres unitats de negoci basades en la base de clients objectiu. La realització de pressupostos és una matriu complexa que abasta totes les unitats de negoci i funcions.
- L' empresa considera la major part de la TI com una fuita de capital o un centre de cost
- A través del Centre de Control l'empresa opera en temps real i de manera automàtica més de 17.000 quilòmetres de xarxes.

- Tots els empleats opten al lloc de treball mitjançant unes oposicions de caràcter administratiu.

Revisada la situació descrita, respon a les següents qüestions:

1. *Amb l' escenari presentat identificar els punts significatius de context que haurà de considerar el nou CISO.*
2. *Relació ordenada de passos per donar resposta a l' estratègia de la companyia.*
3. *Quin creieu hauria de ser l'objectiu final del nou CISO i com s'hauria de materialitzar per garantir i justificar els resultats davant la direcció de la companyia?*
4. *Definir un quadre de comandament que identifiqui el nivell de compliment ENS 2 de l'empresa?*

Mètode de valoració: Total punts 20

1. *Amb l' escenari presentat identificar els punts significatius de context que haurà de considerar el nou CISO.*

   (5p) – Els punts s'assignaran en funció de:

X > 10 factors	100% dels punts
7< X < 10 factors	50 % dels punts
4 < X < 7 factors	25 % dels punts
X < 4 factors	0 % dels punts

   - *Sector*
   - *Àmbit geogràfic*
   - *Volum població abastida*
   - *Model de creixement*
   - *Incorporació d'un CDO*
   - *Interès millora tecnològica*
   - *Shadow IT*
   - *Reducció pressupostària en els propers 5 anys*
   - *Obligació d'acompliment RGPD, NIS, ENS*
   - *Intenció d'anar al núvol*
   - *....*

2. *Relació ordenada de passos per donar resposta a l' estratègia de la companyia.*

(5p) – Els punts s'assignaran en funció de:

Identificació de tots els passos de forma ordenada amb justificació	entre el 80% 100% dels punts
Identificació de part dels passos amb justificació	25% - 80% dels punts
Identificació part dels passos sense justificació	0% - 25% dels punts

- *FASE de Diagnòstic*
  - *Anàlisi intern*
  - *Anàlisi extern*
  - *Anàlisi DAFO*
- *FASE de formulació estratègica*
  - *Aspiració estratègica*
  - *Definició d'eixos, línies i objectius estratègics*
  - *Definició de les fitxes de les iniciatives*
  - *Priorització de les iniciatives/programes*
- *FASE de Desplegament*
  - *Definició d'un pla d'implementació*
  - *Definició d'un QdC de seguiment del pla*

3. *Quin creieu hauria de ser l'objectiu final del nou CISO i com s'hauria de materialitzar per garantir i justificar els resultats davant la direcció de la companyia?*

(5p) – Els punts s'assignaran en funció de:

Identificació d'un objectiu clar i justificat amb descripció clara del mètode de materialització	80% - 100% dels punts
Identificació d'un objectiu no principal i una descripció del mètode de materialització	25% - 80% dels punts
Identificació d'un objectiu sense justificació i una descripció del mètode de materialització	0% - 25% dels punts

- *Crear un model de gestió de la ciberseguretat i explicar-ho de forma clara a la direcció*
- *S'ha de crear un SGSI*
- *Descriure d'un sistema de gestió de la seguretat d'informació (components, interrelació,..)*

4. *Definir un quadre de comandament que identifiqui el nivell de compliment ENS 2 de l'empresa?*

(5p) – Els punts s'assignaran en funció de:

Identificació de tots els àmbits i un % superior al 60% d'indicadors	80% - 100% dels punts
Identificació de part dels àmbits i un % inferior al 60% d'indicadors	25% - 80% dels punts
Identificació d'un objectiu sense justificació i una descripció del mètode de materialització	0% - 25% dels punts

- *Crear un QdC amb els àmbits de gestió de l'ENS amb el corresponents indicador*