Plans de Contingència de TI

Assegurar la disponibilitat

www.abast.es

A mesura que les organitzacions depenen més i més de la tecnologia, que s'ha convertit en un component clau de la major part dels processos de negoci, la disponibilitat dels serveis de TI és imprescindible per a la seva supervivència. Aquesta disponibilitat s'aconsegueix mitjançant la definició i implementació d'un Pla de Contingència l'objectiu del qual consisteix a garantir que es pot recuperar la infraestructura de TI que suporta aquests serveis dins dels terminis i amb el nivell de servei acordat i necessari per al negoci.

Beneficis

1. Reducció d'aquells riscos que, en cas de materialitzar les amenaces que els originen, poden representar pèrdues ingents de capital, bé per facturació fallida, per reposició dels danys causats, per pèrdua d'oportunitat de negoci, per reclamació de clients, per sancions legals , etc.

2. Estalvi de temps i diners a l'afrontar i corregir situacions nefastes abans que ocorrin i ens obliguin a resoldre-les amb presses i a qualsevol preu.

3. Millora de la imatge i revalorització de la confiança en l'empresa dels accionistes, inversors, empleats, proveïdors i clients al mostrar-los que es prenen mesures diàries per garantir la continuïtat del negoci.

Retorn de la inversió

La nostra metodologia té com a objectiu principal ajudar a l'organització a garantir que s'implementen les mesures i estratègies de recuperació que el negoci realment necessita i pot permetre's.

És fonamental, per tant, entendre que significa per al negoci la no disponibilitat dels seus sistemes i realitzar les accions i plans necessaris per evitar que passi. La clau per aconseguir aquesta comprensió és la qualificació (la validació amb el negoci) del que significa realment el temps d'inactivitat i, a continuació, la quantificació (mesurament) de les conseqüències per al negoci. Es tracta, per tant, d'estimar el cost de millorar la infraestructura de TI actual enfront de les pèrdues per no disponibilitat.

Per què ABAST?

La realització de plans de contingència necessita, a més d'un component metodològic o procedimental, un fort component tecnològic. Quan un client aborda un projecte de pla de contingència amb nosaltres, tota la nostra organització treballa per a vostè. El nostre equip de consultors coordina la resta dels nostres departaments tècnics especialitzats que participaran en l'anàlisi de la seva infraestructura tecnològica actual.

Els nostres consultors i tècnics estan altament qualificats i certificats en diverses metodologies i productes amb el compromís d'oferir als seus clients la màxima qualitat en els seus projectes.

La nostra metodologia

1. Anàlisi d'impacte en el negoci. Consisteix a identificar els processos més crítics del negoci, els serveis de TI que els suporten, determinar l'impacte si un o varis d'aquests serveis de TI es veuen afectats totalment o parcialment i definir els requeriments de recuperació establerts pel negoci (temps màxim d'interrupció i màxima pèrdua de dades permesa).

2. Anàlisi de riscos. Consisteix en estimar el risc potencial a què estan sotmesos els sistemes de TI, avaluant l'impacte associat a la materialització d'una amenaça, i definir aquelles recomanacions o controls preventius que permetin reduir o eliminar aquest risc.

3. Definició de les estratègies de recuperació. Consisteix a establir els escenaris de recuperació en funció de les amenaces determinades en l'anàlisi de riscos i els requeriments de negoci definits en l'anàlisi d'impacte.

   En aquesta fase es definirà l'escenari tecnològic òptim per suportar els processos de negoci, atenent a les disponibilitats del servei.

4. Desenvolupament i implementació del Pla de Contingència. Un cop definida l'estratègia de recuperació, el pla ha de definir i establir els procediments, manuals tècnics i checklists funcionals que permetin restaurar els serveis de TI (sistemes, operacions i dades) després d'una emergència o afectació total o parcial d'aquests serveis. La implementació del pla consisteix en l'execució de les recomanacions establertes en l'anàlisi de riscos i l'escenari tecnològic definit.

5. Prova i manteniment del pla. Les proves del pla són essencials per identificar les deficiències de planificació i preparació de personal. A més, el pla ha de ser un document viu que s'actualitza periòdicament per mantenir-se a el dia amb els canvis en els sistemes de TI.

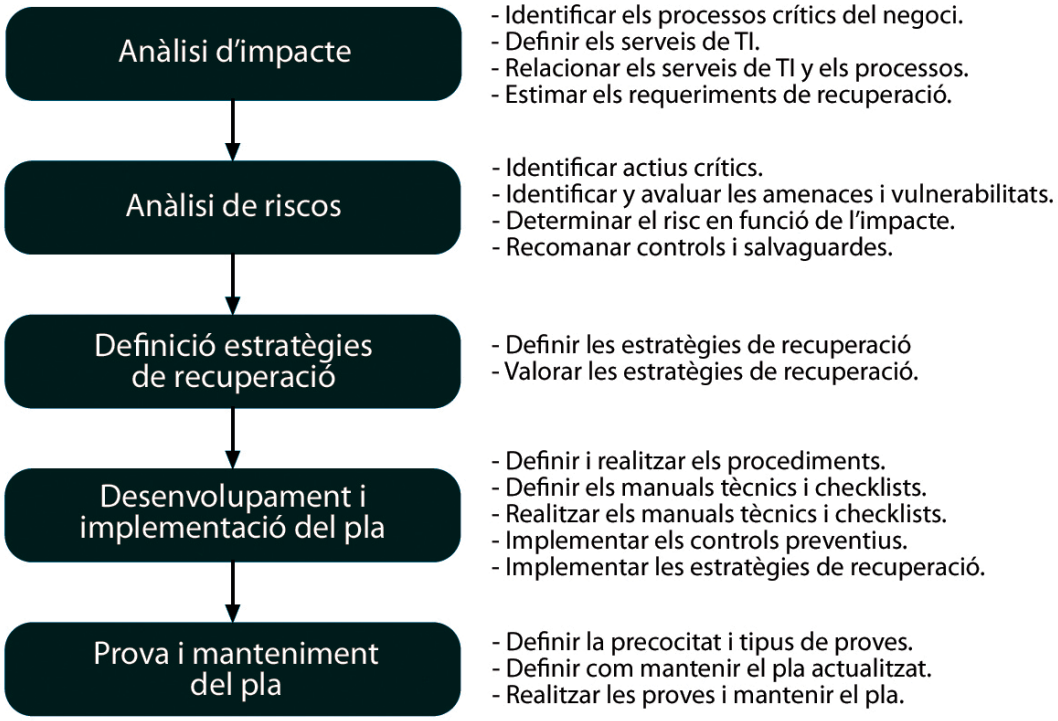
CYBALL. Serveis de seguretat global d'Abast

ABAST ofereix una àmplia oferta de serveis i solucions per donar resposta a les seves necessitats en ciberseguretat i seguretat del negoci. Les estructurem en 4 capes:

- GOVERN: Alineació estratègica seguretat / negoci. Tractament del risc. Anàlisi cost / benefici. Mesura de la maduresa de la seguretat.
- GESTIÓ: Auditories de Seguretat. Continuïtat de negoci. Compliment normatiu / legal. Gestió de crisi i d'incidències. Formació i conscienciació.
- OPERACIONS (SOC / MDR): Monitorització de la Seguretat 24x7. Detecció d'Amenaces i incidents. Prevenció de bretxes. Resposta als incidents.
- INFRAESTRUCTURA: Assessorament i implantació d'infraestructura / solucions de seguretat TI. Administració de la seguretat TI.

abast cyball 360°

Fases d'un pla de contingència de TI



Para más información:
seguridad@abast.es