Seguretat Informàtica

Index

Polítiques de backup

→ Servidor Zentyal i Windows

Referent a les copies de seguretat utilitzarem el següent model per el servidor Zentyal i un dels Windows, encarregat de les copies de seguretat;

Dilluns	Dimarts	Dimecres	Dijous	Divendres	Dissabte	Diumenge
1 Copia total. Disc 1.	2 Copia incremental.	3 Copia incremental.	4 Copia incremental.	5 Copia total.Disc extern.	6	7
8 Copia incremental.	9 Copia incremental.	10 Copia incremental.	11 Copia incremental.	12 Copia total.Disc extern.	13	14
15 Copia incremental.	16 Copia incremental.	17 Copia incremental.	18 Copia incremental.	19 Copia total.Disc extern.	20	21
22 Copia incremental.	23 Copia incremental.	24 Copia incremental.	25 Copia incremental.	26 Copia total.Disc extern.	27	28
29 Copia incremental.	30 Copia total.Disc 1 i extern.					

El dia 1 de cada mes farem una copia total i al final de mes també. Es farà tant al disc dur intern com en el extern.

- Per al Zentyal tindrem el disc dur del ordinador i dos disc durs externs.
- Per al Windows disposem del disc dur del ordinador i un disc dur extern.

On posa disc 1 es el disc dur del ordinador i on posa extern son els disc durs externs.

Els disc durs externs, no hi seran a la empresa, dos components dels equips es portaran cada un el seu a casa seva.

Ho farem de aquesta manera perquè així només es guardara la informació que falti des de la ultima copia, es a dir, el dia 1 Dilluns, farem una total i a partir de aquí en farem una incremental cada dia,aixi Dimarts guardara lo que s'hagi modificat partint de la copia de l'anterior dia.

Les copies començaran a partir de les 21:00 de la nit, donant temps a que es pugi tenca la botiga en cas d'imprevist o durada de atenció a un client.

Les dades que emmagatzem dels ordinadors dels clients només les tindrem durant dugues setmanes. Un cop finalitzat aquest plaç les dades seran eliminades del sistema principal, es a dir, del disc dur intern del ordinador del Windows 7. Les del disc dur extern les tindrem emmagatzemades durant 1 mes per si passa alguna cosa al ordinador del client. Transcorri't aquest temps no ens fem càrrec de les pèrdues de les dades.

→ Altres ordinadors de la empresa.

Referent a l'altre windows i al ubuntu les dades que contenen aquest dos equips no son tan 'importants' com el servidor o el Windows encarregat de les copies de seguretat asi que el que farem serà es;

- Copia total principi i final de cada mes en el disc dur 1.
- Copia incremental cada Dimecres i Divendres.

SAI

Què es?

Es un aparell elèctric que subministra energia elèctrica quan la font primària d'electricitat falla.

Ús:

L'ús habitual d'un SAI és per protegir qualsevol equipament en què una baixada de tensió pugui provocar danys al propi equipament o a qualsevol cosa que pugui dependre d'aquest equipament. Entre els usos més comuns es troben els ordinadors, centres de dades i l'equipament de telecomunicacions.

Diferencia de SAI i generador:

Es diferencien perquè el SAI actua immediatament quant es produeix la caiguda gracies a l'energia que té emmagatzemada en les bateries.

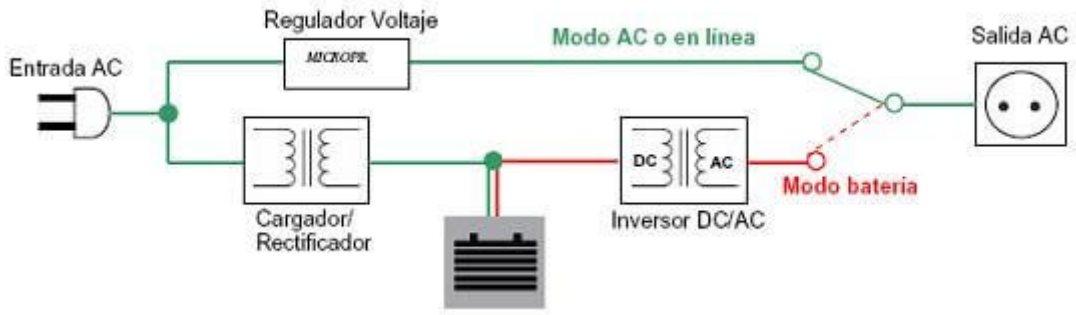
Temps de durada:

Encara que el temps en què proveeix d'energia elèctrica és relativament curt, normalment es suficient per a poder guardar el que se estava fent en aquell moment.

SAI per a l'empresa:

Tindrem un ***SAI INLINE*** o SAI interactiu.

Es semblant al SAI OFFLINE però incorpora un microprocessador que controla les fluctuacions de la xarxa en ± 15% , regulant la tensió de sortida. Aquest procés de filtrat i millora contínua del corrent que arriba als dispositius connectats al SAI, es realitza sense que entrin a funcionar les bateries, de manera que la protecció amb un SAI interactiu és més gran encara sense patir apagades . En el moment en què es detecta un tall de corrent comencen a funcionar instantàniament les bateries per evitar que l'ordinador s'apagui .



Raid

Considerem que, al tenir la política que tenim de copies de seguretat i d'emmagatzemament de dades, les nostres dades estan segures, integres i protegides contra les possibles fallades del sistema.

Com heu vist tenim més d'una copia i no es troben totes al mateix lloc, el disc durs dels ordinadors son bastant potents i capaços de durar temps.

Som una empresa petita-mitjana per lo qual no tenim tant volum de dades ni tanta 'necessitat' de tenir un d'aquests elements .

LOPD

Què es?

'Ley de Protección de Datos' , és una llei orgànica que té com a objectiu garantir i protegir les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment la seva intimitat i privadesa personal i familiar.

Obligacions

- Inscripció de fitxers en la 'Agencia de Protección de Datos'.
- Legitimar les dades personals mitjançant els següents principis;
    * Principi del consentiment del client/afectat.
    * Principi d'informar al afectat/client del que com farem amb les seves dades.
    * Principi de la qualitat de les dades.
- Protegir els arxius (tant informàtics com en paper) per a reservar la confidencialitat,integritat i disponibilitat de les dades .
- Deure de secret.
- Fer complir els drets ARCO.

Aspectes bàsics requerits:

- Disposar de un Document de Seguretat.
- Definí e implantar els procediments requerits.
- Escollir un Responsable de seguretat.
- Formar i fer entendre al personal sobre el tema de seguretat de la informació de manera que tinguin en compte tots els aspectes sobre la seguretat de les dades.

S'ha de tenir molt en compte els següents articles de la normativa;

Art 101.2. Xifratge de dades .
La distribució dels suports que continguin dades de caràcter personal es realitzarà xifrant aquestes dades garantint que aquesta informació no sigui vista ni manipulada durant el seu transport. L'encriptació recomanada es el xifratge de 128 bits.

Art 103. Registre d'accés.
L'administrador no té accés a les dades excepte autorització expressa del client. En el cas de necessitar executar una recuperació en el data-center, l'usuari ha de proporcionar la seva clau de seguretat. L'accés queda registrat.

Art 102. Copies de seguretat en un lloc diferent aquell on es troben els equips informàtics.
És la funcionalitat principal de les nostres eines de backup online. Obligatori en les còpies per a la protecció de dades d'alt nivell.

Art. 104. Transmissió de dades per xarxes de Telecomunicacions .
Les dades es transmeten, xifrats i comprimits, sota un protocol de comunicació segur SSL (https).

Art. 94.2. Verificació periòdica de la còpia .
El responsable del fitxer s'encarregarà de verificar cada sis mesos la correcta definició, funcionament aplicació dels procediments de realització de còpies de respatller i de recuperació de les dades.

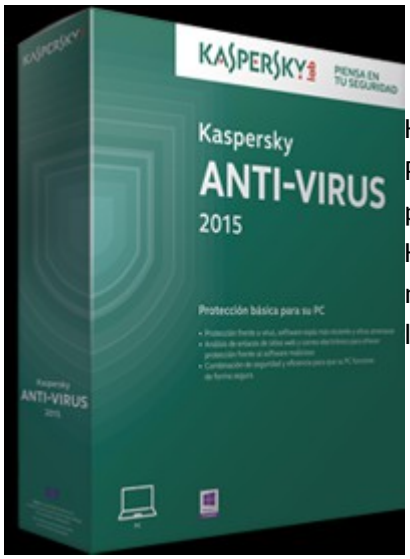
Que son els drets ARCO?

Són el conjunt de drets a través dels quals la llei orgànica 15/1999 de Protecció de Dades de Caràcter Personal (LOPD) garanteix a les persones el poder de control sobre les seves dades personals.

DRETS ARCO	
Dret de informació	Al moment en què es procedeix a la recollida de les dades personals, l'interessat ha de ser informat prèviament de manera expressa, precís i inequívoc de, entre uns altres, l'existència d'un fitxer, de la possibilitat d'exercitar els seus drets i del responsable del tractament.
Dret d'accés	Permet al ciutadà conèixer i obtenir gratuïtament informació sobre les seves dades de caràcter personal sotmesos a tractament.
Dret de rectificació	Es caracteritza perquè permet corregir errors, modificar les dades que resultin ser inexactes o incomplets i garantir la certesa de la informació objecto de tractament.
Dret de cancel·lació	Permet que se suprimeixin les dades que resultin ser inadequats o excessius sense perjudici del deure bloquejo recollit en la LOPD.
Dret de oposició	És el dret de l'afectat al fet que no es dugui a terme el tractament de les seves dades de caràcter personal o se cessi en el mateix.

Protecció contra software maliciós

La nostre empresa per protegir-se del software maliciós i altres amenaces que hi han utilitzarem el següent;



Anti-Virus Kaspersky;

Kaspersky Anti - Virus 2015 és la primera arma de defensa del teu PC i t'ofereix tecnologies antimalware guardonades que et protegeixen enfront de virus , spyware i altres tipus de malware . Kaspersky Anti - Virus 2015 , que s'ha optimitzat per garantir el millor rendiment , funciona en segon pla i et protegeix enfront de les amenaces més recents sense alentir teu PC.

Avast;

Avast! Free Antivirus és el programari gratuït de la versió d'Avast! antivirus, és només disponible per a ús personal, i no comercial, i està disponible per Linux, Windows, Mac OS i Android mentre que *Avast! Antivirus Pro* ofereix una protecció i característiques addicionals per a empreses i professionals. **Avast!** també incorpora un escàner de línia i una escriptura bloquejadora.

En el servidor a més a més comptarà amb el seu propi antivirus, que es dins del paquet Zentyal.

Pla de contingència

- **Introducció**

Un Pla de Contingència es un conjunt de "Activitats" que busquen definir i complir metes que permetin a cada departament de una empresa ,en aquest cas a EDDA CODE, controlar el risc associat a una contingència.

- **Planificació del Pla de contingència**

Aquest pla esta orientat a establir amb els treballs de seguretat,un sistema adequat de seguretat física i lògica en previsió de desastres.

Es defineix la *Seguretat de Dades Informàtics* com un conjunt de mesures destinades a salvaguardar la informació contra els danys produïts per fets naturals o per l'home.

S'ha considerat que per a l'empresa, la seguretat es un element bàsic per garantir la seva supervivència i per tant, considera la Informació com un els actius més importants de l'Organització, la qual cosa fa que la seva protecció, sigui el fonament més important d'aquest Pla de Contingència.

Les mesures considerades en aquest document son:
- Anàlisi de risc.
    Dades importants
    Bens susceptibles a danys
    Tipus de risc
    Danys i fonts de danys
- Mesures preventives.
- Anàlisi i Avaluació de danys
- Pla d'acció .
- Temps de recuperació.

- **Anàlisis de risc**

En aquest apartat identificarem els objectes que han de ser protegits,els danys que poden patir, les seves possibles fonts de dany . Aixi com la manera de minimitzar els danys.

→ Dades més importants

- Software
- Hardware
- Dades

→ Bens susceptible a danys:

- Hardware i software (servidor,ordinadors,etc)
- Dades e informació (documentació de la empresa i dades dels clients)
- Instal·lació (elèctrica, d'aigua, establiment/local)
- Personal
- Altres bens (tintes, memòries ram,etc.)

→ Tipus de risc:

- Ambientals: factors externs, pluges,inundacions, tormentes, llamps, brutícia, humitat, calor,...
- Tecnològics: errades de hardware i/o software,errades en el servei elèctric, atacs per virus informàtics, etc.
- Humans: furts, modificacions/ pèrdua de dades, sabotatge, vandalisme, crackers, hackers, falsificació,robatori de contrasenyes, intrusions, alteracions,

→ Danys i fonts de danys:

Accés no autoritzat:
- Impossibilitat d'accés als recursos ; ja sigui per causes de problemes físics, a les instal·lacions, o lògics , no poder entrar al ordinador per canvi de claus o programari maliciós que l'ha infectat.
- Instal·lació de programari de comportament erràtic i / o nociu per a l'operació dels sistemes computacionals en ús .
- Robatori, pèrdua de material.

Desastres Naturals:
- Inundacions causats per falla en els subministraments d'aigua.
- Per falles de la xarxa d'energia elèctrica pública per diferents raons alienes al maneig per part de la Companyia.

Falles de Maquinari
- Falla al Servidor d'Aplicacions i Dades, tant en el seu (s) disc (s) dur (s) com en el processador central.
- Falla al maquinari de Xarxa: Falla en els Switches, al cablejat de la Xarxa, el Router, el Firewall.

Altres:

- Quedar-se sense internet per falles de Central Telefònica .
- Incendis.
- Falles de personal clau. (Es considera personal clau aquell que compleix una funció vital en el flux del proces de dades o operació dels Sistemes d'Informàtics) .

- **Mesures Preventives:**

- Restringir l'accés a les àrees de ordinadors importants.
- Instal·lar detectors de fum i extintors (foc).
- Establir vigilància mitjançant càmeres de seguretat en el lloc.
- Col·locar els dispositius enlairats del sòl (agua).
- Col·locar els dispositius lluny de les finestres (pluja).
- Determinar llocs especials, fora del centre de dades, per emmagatzemar-mitjans magnètics de seguretat i còpia de la documentació diferencia i procediments de seguretat i recuperació.
- Software anti-virus, firewall.
- SAI.
- Software/Hardware de detecció d'errades.

- **Anàlisi i Avaluació de d'anys**

→ En cas de que no sigui possible començar immediatament les operacions s'haurà de procedí de la manera següent:

- Recollir els suports de dades, programes, manuals i claus del lloc en el que es trobin resguardades. Responsable: Judith Gutiérrez

- Si les falles es deriven del mal funcionament d'un equip (maquinari) es procedeix al seu reemplaçament immediat. Responsable: Judith Gutiérrez

- Instal·lar el sistema operatiu. Responsable: Judith Gutiérrez
- Restaurar la informació de les bases de dades i programes. Responsable: Edgar Ordoñez .
- Revisar i provar la integritat dels dades. Responsable: Edgar Ordoñez.
- Iniciar les operacions.

→ En els casos en què l'alteració pot ser corregida sense problemes greus, es procedeix d'acord amb el següent:

- Correcció de les alteracions que es localitzin en els servidors Hardware. Responsable: Judith Gutiérrez.
- Correcció de les alteracions que es localitzin en els servidors Software. Responsable: Edgar Ordoñez.
- Revisió i prova de la integritat de les dades. Responsable: Edgar Ordoñez.
- Iniciar les operacions

- **Pla d'acció**

1. Inventari dels serveis informàtics.
Dur a terme un inventari d'equip de còmput, programari i mobiliari, per determinar quina és la informació crítica que s'ha de protegir.
2. Identificar els tipus de sinistres als quals està propens cadascun dels processos crítics.
3. Identificar el conjunt d'amenaces que poguessin afectar els processos informàtics, ja sigui per causa accidental o intencional.
4. Revisar la seguretat.
S'ha d'estar preparat per a qualsevol contratemps, verificant que dins l'empresa es compti amb els elements necessaris per salvaguardar els seus actius.
5. Identificar els serveis fonamentals de l'àrea de sistemes informàtics de l'empresa (Factors Crítics).

- **Temps de recuperació**

Depenent del tipus de contingència durara un temps o un altre, si mirem aquesta taula veurem mes o menys lo que es trigaria;

Tipus	Definició	Hores
Lleu	Repercussió en la operació diària.	8 hores
Greu	Danys a les instal·lacions.	24 hores
Molt Greu	Afecta a la operació i a les instal·lacions, no es recuperable a curt plaç. (per desastre.)	---

Pressupost

Aquí es contemplarà el que hem invertit en la nostra política de seguretat, en el pla de contingència.

EDDA CODE PLA CONTINGENCIA PRESSUPOST FINAL	
Càmeres de vídeo vigilància i alarmes	200 €
Claus del local	5'18 €
Detectors de fums	9 €
Extintors	65 €
Mobiliari	900 €
Moble Rack	359 €
Antivirus	39'95 €
SAI	321 €
Zentyal Enterprise* (Servidor extern de emmagatzematge de dominis,dades i copies de seguretat al nuvol)	99'50 €
Discos durs externs	215,92 € (53'98 x 4)
TOTAL	2214,55 €

Cas de pèrdua de dades

→ Cas 1; Pèrdua de dades en el windows encarregat de les copies dels clients

- Per virus encriptat
Aquest tipus de virus que encripten les dades son molt difícils de treure , en cas que no pugéssim treure'l no seria per tant, ja que amb la nostra política de copies de seguretat podríem passar les dades de un dels disc durs externs que tenim .
- Per que el disc dur del ordinador esta xafat
En aquest cas, igual que en el anterior , no es cap problema. Agafaríem un disc dur nou copiaríem la imatge del sistema que tenim de aquest ordinador i en cas de que falti alguna dada es passa de un dels disc durs externs.

→ Cas 2; Caiguda del servidor

Es poc provable pro en cas de que el nostre servidor caigui tenim un SAI que alimentara lo suficient per a poder guardar lo ultim que s'ha fet.
I si falles el seu disc dur tenim copies de seguretat fetes que podrem restaurar en cas de aquest tipus de fallada o de una altre.

Per el servei de Hosting que oferim tampoc es tant greu ja que esta subcontractat amb Zentyal i esta enllaçat als seus servidors.
En cas de caiguda de el servidor de Zentyal tindrem una copia de seguretat de les dades de les webs que tenim al nostre hosting.

Procediment de recuperació de dades

Vídeo en el canal de la empresa:
https://www.youtube.com/channel/UCx3XVzZRnBdTtDMf25xip5g