16 de novembre de 2023

Generació de continguts IA - Seguretat i privacitat II

ImpacTech

Innovació i Tecnologia
per la transformació social

Introducció

De què parlarem avui?

ImpacTech

Bon dia, avui explorarem com la seguretat i la privacitat digital es converteixen en claus fonamentals per a les entitats dins de l'Economia Social i Solidària (ESS). En un món on la informació digital es mou ràpidament i on cada cop més processos es duen a terme de manera electrònica, les nostres organitzacions no poden quedar al marge d'aquesta evolució. La nostra missió, valors i objectius socials es veuen directament afectats per com gestionem aquestes noves eines tecnològiques.

De què parlarem avui?

Aquesta sessió està dissenyada per proporcionar-vos els coneixements i eines necessàries per protegir la vostra informació i la de les persones amb qui treballeu.
Entendre i aplicar mesures de seguretat i privacitat no és només una qüestió tècnica, sinó també una extensió dels nostres principis de responsabilitat, transparència i solidaritat.

Principis de l'ESS i la Protecció de Dades

ImpacTech

En l'ESS, els principis van més enllà del benefici econòmic. Es prioritza el benestar de les persones i el medi ambient, la cooperació i el treball col·lectiu. Aquest enfocament humanista també s'ha de reflectir en com es tracten les dades personals i confidencials. Protegir aquesta informació és fonamental per mantenir la confiança i la integritat dins de les vostres comunitats.

Desafiaments i Oportunitats

Les amenaces a la seguretat digital, com els ciberatacs o el robatori de dades, són riscos reals que poden tenir conseqüències greus. Però, al mateix temps, una bona gestió de la seguretat i la privacitat pot ser una oportunitat per destacar la nostra responsabilitat social i reafirmar el compromís amb els valors de l'ESS. Això ja ho vam veure a la sessió de política de gestió del coneixement.

ImpacTech

Innovació i Tecnologia
per la transformació social

Fonaments de Seguretat i Privacitat

Definició i Importància

ImpacTech

La seguretat de la informació es refereix a la protecció de dades digitals i físiques de l'accés no autoritzat, l'ús, la divulgació, la interrupció, la modificació, la inspecció, l'enregistrament o la destrucció. És crucial per mantenir la confidencialitat, la integritat i la disponibilitat de la informació, especialment en organitzacions de l'ESS on la gestió de dades confidencials és habitual.

Principis Clau

ImpacTech

- **Confidencialitat:** Cal assegurar que la informació és accessible només per a aquelles persones autoritzades.
- **Integritat:** Mantenir la precisió i la totalitat de les dades.
- **Disponibilitat:** Garantir que la informació i els recursos relacionats estan disponibles quan són necessaris.

Mesures de Seguretat

ImpacTech

Exemples de mesures de seguretat: firewalls, antivirus, autenticació de dos factors, còpies de seguretat regulars, etc.

Seguretat Física i Medis de Control

ImpacTech

- **Control d'Accés Físic:**
  - Instal·lació de sistemes de seguretat com alarmes, càmeres de vigilància i controls d'accés per limitar l'entrada a zones on es gestionen dades confidencials.
  - Establir protocols per a visitants i mantenir un registre d'entrada i sortida.
- **Protecció contra Desastres Naturals i Incendis:**
  - Implementació de sistemes antiincendis i plans de contingència per a desastres naturals.
  - Assegurar una bona ubicació i aïllament dels equips informàtics per minimitzar el risc de danys.

- **Firewalls i Sistemes Anti-malware:**
  - Instal·lació i actualització regular de firewalls i programes anti-malware per protegir contra virus, worms, troians i altres amenaces digitals.
  - Configuració dels firewalls per controlar el trànsit d'entrada i sortida a la xarxa.
- **Gestió de Patches i Actualitzacions:**
  - Mantenir tots els programes i sistemes operatius actualitzats amb els últims patches de seguretat.
  - Automatització de les actualitzacions quan sigui possible per assegurar la implantació ràpida de correccions de seguretat.

- **Autenticació Forta i Gestió de Contrasenyes:**
  - Implementació d'autenticació de dos factors o multifactor per accedir a sistemes sensibles.
  - Polítiques de contrasenyes fortes (longitud, complexitat, renovació periòdica).
- **Xifrat de Dades:**
  - Utilització de xifratge en la transmissió i emmagatzematge de dades confidencials.
  - Xifrat de dispositius mòbils i equips portàtils per protegir les dades en cas de pèrdua o robatori.

- **Còpies de Seguretat i Recuperació de Dades:**
  - Realització regular de còpies de seguretat de dades crítiques, preferiblement en ubicacions fora de lloc.
  - Pla de recuperació davant desastres per restablir dades i sistemes operatius en cas de pèrdua massiva.
- **Seguretat en Xarxes Sense Fils:**
  - Protecció de xarxes Wi-Fi amb encriptació WPA3 i amagant el SSID per evitar accessos no autoritzats.
  - Limitació de l'accés a la xarxa sense fils a només dispositius autoritzats.

- **Formació i Conscienciació del Personal:**
  - Sessions de formació regulars per al personal sobre pràctiques de seguretat.
  - Informar sobre els riscos de phishing, enginyeria social i altres tàctiques d'atac comunes.

Un procés continu

ImpacTech

Aquestes mesures proporcionen una capa robusta de seguretat per protegir les dades i sistemes de les entitats dins de l'ESS, ajudant a prevenir atacs i a minimitzar el dany en cas que es produeixin. És clau recordar que la seguretat **és un procés continu**, no un estat fix, i requereix una vigilància i actualització constants.

ImpacTech

Innovació i Tecnologia
per la transformació social

Riscos i Amenaces Comunes

Tipus d'Atacs: Phishing, Ransomware, etc.

ImpacTech

Injeccions de codi

Permet injectar codi maliciós a través del lloc web. Els més habituals Cross-Site Scripting i les injeccions SQL

Frau directe

Fan servir targetes robades i ens veiem en l'obligació de retornar els diners.

Clickjacking

Roba les pulsacions d'un teclat o ratolí a un lloc (credencials) per fer-lo servir després.

DDos

Denegació de servei amb un excés de peticions per fer caure la plataforma

Phising

Fan una suplantació de la web per fer-se amb dades dels usuaris.

Robatori informació

Targetes de crèdit, contrasenyes, dades personals són el principal objectiu.

Tipus d'Atacs: Phishing, Ransomware, etc.

ImpacTech

- **Phishing:**
  - **Definició:** Atacs que enganyen les víctimes perquè revelin informació confidencial (com credencials d'accés) mitjançant correus electrònics o llocs web falsos.
  - **Exemples:** Correus electrònics que semblen ser d'entitats de confiança, sol·licitant dades personals o financeres.
  - **Prevenció:** Formació en reconeixement de correus electrònics i missatges sospitosos, no fer clic en enllaços dubtosos.

Tipus d'Atacs: Phishing, Ransomware, etc.

ImpacTech

- **Ransomware:**
  - **Definició:** Programari maliciós que xifra les dades de l'usuari i exigeix un rescat per al seu accés.
  - **Exemples:** Atacs que bloquegen l'accés a dades importants, exigint pagaments per recuperar l'accés.
  - **Prevenció:** Còpies de seguretat regulars, actualitzacions de seguretat, i evitar l'obertura de fitxers adjunts de fonts desconegudes.

Tipus d'Atacs: Phishing, Ransomware, etc.

ImpacTech

- **Atacs a la Xarxa:**
  - Inclouen atacs com l'intercepció de dades (Man-in-the-Middle), l'ús de xarxes Wi-Fi no segures, i els atacs DDoS.
  - **Prevenció:** Utilització de xarxes segures, VPNs, i sistemes de detecció i prevenció d'intrusions.
- **Programari maliciós i Virus:**
  - Programes maliciosos que poden danyar sistemes, robar dades, o alterar el funcionament normal dels equips.
  - Prevenció: Antivirus actualitzats, prudència en la descàrrega de programari, i restriccions en l'ús de dispositius externs.

Possibles Conseqüències d'una Mala Gestió en Seguretat i Privacitat

ImpacTech

- **Pèrdua de Confiança i Reputació:** Un atac exitós pot erosionar la confiança de la ciutadania i altres entitats en l'organització, afectant la seva reputació a llarg termini.
- **Perjudicis Econòmics:** Els costos associats amb la recuperació de dades, les multes per incompliment de lleis de protecció de dades, i la possible pèrdua d'ingressos.
- **Impacte en la Continuïtat del Servei:** Atacs com el ransomware poden interrompre operacions crítiques, afectant la capacitat de l'entitat per servir a la seva comunitat.

Possibles Conseqüències d'una Mala Gestió en Seguretat i Privacitat

ImpacTech

- **Riscos Legals i Compliment:** Incompliment de normatives com el GDPR pot resultar en sancions significatives i litigis.
- **Riscos per a la Seguretat Personal:** La filtració de dades personals pot posar en risc la seguretat i privacitat de les persones afectades.
- **Dany a les Relacions amb Socis i Inversors:** Les conseqüències d'un atac poden afectar la percepció dels socis i inversors, posant en risc les relacions i el finançament.

ImpacTech

Innovació i Tecnologia
per la transformació social

Estratègies de Protecció

Criptografia

ImpacTech

La criptografia és l'art de protegir la informació mitjançant la transformació d'aquesta (coneguda com a xifratge) en un format incomprensible per a qualsevol que no estigui autoritzat a veure-la. Això es realitza utilitzant algoritmes matemàtics complexos i claus secretes. El procés invers, anomenat desxifrat, permet tornar la informació al seu format original utilitzant una clau, que pot ser la mateixa que per al xifratge (criptografia simètrica) o una diferent (criptografia asimètrica).

Protecció Durant la Transmissió

ImpacTech

Quan enviem informació a través d'internet, com en un correu electrònic, una transacció bancària, o fins i tot durant una conversa per xat, la criptografia ajuda a protegir aquestes dades dels ulls indiscrets. Utilitzant el xifratge, la informació s'envia en un format codificat. Només el destinatari correcte, amb la clau de desxifrat adequada, pot convertir aquesta informació de nou en un format llegible. Això és crucial per evitar que els ciberdelinqüents interceptin i utilitzin les dades per a fins maliciosos.

Seguretat en l'Emmagatzematge de Dades

ImpacTech

D'altra banda, la criptografia també es fa servir per protegir les dades emmagatzemades en els nostres dispositius i servidors. Això inclou documents confidencials, registres financers, dades personals dels usuaris, entre altres. En xifrar aquestes dades, assegurem que, fins i tot si un intrús guanya accés físic al dispositiu o al servidor, no podrà entendre ni utilitzar la informació sense la clau de desxifrat.

Importància en l'Economia Social i Solidària (ESS)

ImpacTech

Per a les entitats de l'ESS, que sovint gestionen informació confidencial relacionada amb els seus usuaris, socis i operacions, la criptografia no és només una mesura de seguretat tecnològica, sinó també una pràctica alineada amb els valors de confidencialitat, responsabilitat i confiança. Protegir les dades amb criptografia significa defensar la integritat i la privacitat de les persones i grups amb els quals treballem, reafirmant el nostre compromís amb un treball ètic i segur.

Eines i Pràctiques de Seguretat

ImpacTech

- **Autenticació de Dos Factors (2FA):**
  - Implementació de 2FA com a capa addicional de seguretat per a l'accés a comptes i sistemes crítics.
  - Exemples d'2FA: SMS, aplicacions d'autenticació, i tokens de seguretat físics.
- **Gestió de Contrasenyes:**
  - Ús de gestors de contrasenyes per crear i emmagatzemar contrasenyes fortes i úniques.
  - Polítiques per a la renovació regular de contrasenyes i l'ús de frases de contrasenya.

Eines i Pràctiques de Seguretat

ImpacTech

- **Seguretat en Xarxes i Comunicacions:**
  - Protecció de xarxes mitjançant tallafocs, VPN, i sistemes de detecció d'intrusions.
  - Fomentar l'ús de xarxes Wi-Fi segures i la prudència en l'ús de xarxes públiques.
- **Actualitzacions i Pegats de Seguretat:**
  - Mantenir els sistemes i aplicacions actualitzats per protegir-se contra vulnerabilitats conegudes.
  - Implementació de polítiques per a l'actualització automàtica de programari.

ImpacTech

Innovació i Tecnologia
per la transformació social

5 claus per la vostra seguretat

ImpacTech

1

Fer servir plataformes segures

És important veure que ofereix cada plataforma, si permet monitorar, fer prevenció de frau...

2

Certificats SSL

Ja ho hem comentat abans, els certificats SSL són claus per la seguretat a la web. A més proporciona confiança a l’usuari.

3

Tenir formes de pagament /cobrament segures

Comptar amb solucions com PayPal o passarel·les de pagament d’entitats bancàries.

ImpacTech

4

Compte al guardar dades confidencials

Guarda només la informació que sigui necessària.

5

Actualitzar

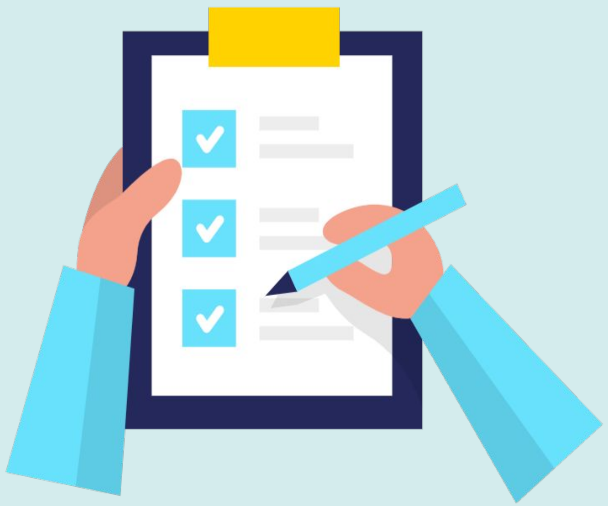
Teniu sempre la vostra plataforma, els connectors, les vostres eines digitals actualitzades sempre.

Més claus per augmentar la vostra seguretat

ImpacTech

- Fer servir contrasenyes segures
- Utilitza mètodes d'autentificació de doble factor
- Sospita de missatges estranys que et puguin fer arribar coneguts.
- Compte amb enllaços desconeguts.
- Estigues previngut dels atacs d'enginyeria social

Quines més podem posar a la llista?



ImpacTech

Innovació i Tecnologia
per la transformació social

Conclusions

Conclusions

ImpacTech

- **Importància de la Seguretat i la Privacitat:** Hem vist com la seguretat i la privacitat són fonamentals en el context de l'Economia Social i Solidària. Protegir les dades no només és una qüestió legal, sinó també un compromís ètic i un element clau per a la confiança i la integritat de les nostres organitzacions.
- **Riscos i Estratègies de Protecció:** Hem identificat els principals riscos, com el phishing i el ransomware, i com aquests poden afectar les nostres entitats. A més, hem explorat diverses estratègies i eines per mitigar aquests riscos, incloent-hi la criptografia, la gestió de contrasenyes, i les polítiques de privacitat.

Conclusions

ImpacTech

- **Cultura de Seguretat:** És essencial fomentar una cultura de seguretat dins de les nostres organitzacions, on cada membre estigui informat, capacitat, i compromès amb la protecció de les dades.
-

ImpacTech

Innovació i Tecnologia
per la transformació social

Recursos

Conclusions

ImpacTech

- Webs i Blogs Especialitzats:
  - Agència de ciberseguretat de Catalunya: https://ciberseguretat.gencat.cat/ca/inici
  - Internet Segura: https://xtec.gencat.cat/ca/recursos/tecinformacio/internet_segura/
- Cursos i Formacions Online:
  - Curs online seguretat a la Xarxa - Barcelona Activa: https://cibernarium.barcelonactiva.cat/ficha-actividad?activityId=998430

Conclusions

ImpacTech

- Publicacions i Guies:
  - Privacidad y seguridad en internet: https://www.aepd.es/documento/guia-privacidad-y-seguridad-en-internet.pdf
  - Guía de ciberseguridad - INCIBE: https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberseguridad-la-ciberseguridad-al-alcance-de-todos