La ciberseguretat a les entitats

2024

Guia

Generalitat de Catalunya
Departament de Cultura

Amb el suport del Departament de Cultura de la Generalitat de Catalunya.

Fundesplai
Fundació Catalana de l'Esplai

Què és la Ciberseguretat?

Introducció

En un món cada vegada més digitalitzat, les entitats del tercer sector s'enfronten a nous reptes en matèria de ciberseguretat. Sovint les entitats gestionen dades sensibles de persones beneficiàries, de donants, del voluntariat i altres col·lectius amb qui es relacionen. **En el marc de les seves activitats sovint les entitats són vulnerables davant de la ciberdelinqüència, que intenta aprofitar-se de la manca de recursos tècnics i humans destinats a la seguretat digital.**

Un incident de ciberseguretat pot tenir conseqüències greus com ara:

- Pèrdua de dades personals
- Interrupcions en els serveis oferts
- Danys a la reputació
- Sancions econòmiques per l'incompliment de normatives com ara el RGPD

Per això, és essencial que les entitats desenvolupin una estratègia de ciberseguretat adequada a la seva realitat i capacitats.

Principis bàsics de ciberseguretat

La ciberseguretat fa referència al conjunt de mesures, pràctiques i eines destinades a protegir les dades, sistemes i xarxes digitals contra possibles amenaces. Això inclou evitar accessos no autoritzats, protegir la informació confidencial i garantir que els serveis digitals funcionin sense interrupcions.

Per a les entitats del tercer sector, la ciberseguretat és especialment important perquè sovint treballen amb dades sensibles de persones vulnerables i qualsevol incident pot tenir un gran impacte social i econòmic.

Amenaces comunes

Les entitats del tercer sector, com qualsevol altra organització, estan exposades a diversos riscos digitals, que es poden derivar de vulnerabilitats internes, com ara la manca de formació o recursos, o bé d'atacs externs dirigits. Algunes de les situacions més habituals inclouen:

- **Phishing**: correus electrònics o missatges enganyosos que intenten obtenir informació confidencial, com ara contrasenyes o dades bancàries.
- **Ransomware:** atacs que bloquegen l'accés a la informació i exigeixen un rescat per recuperar-la.
- **Malware**: programes maliciosos que poden danyar els sistemes o robar informació.

- **Accés no autoritzat**: persones que aconsegueixen entrar als sistemes de l'entitat mitjançant contrasenyes febles o vulnerabilitats en els sistemes.

Bones pràctiques generals

Per començar a millorar la seguretat digital, les entitats poden adoptar mesures que són senzilles d'implementar i molt eficaces. Algunes d'aquestes mesures són:

- **Utilitzar contrasenyes robustes i segures**. Això significa evitar contrasenyes simples com "123456" o "admin", utilitzar combinacions de lletres, números i símbols amb una longitud mínima de 12 caràcters, i canviar-les periòdicament sense reutilitzar-ne cap d'antiga.
- **Mantenir els sistemes actualitzats** és clau per protegir-se de vulnerabilitats conegudes. Tots els programes i sistemes operatius han d'estar actualitzats amb les darreres versions de seguretat disponibles, i és molt recomanable configurar les actualitzacions automàtiques sempre que sigui possible.
- **Realitzar còpies de seguretat periòdiques.** Aquestes còpies han de contenir les dades més importants i emmagatzemar-se en llocs segurs, preferiblement fora de línia o al núvol, per garantir-ne la recuperació en cas d'incident.
- **Sensibilitzar l'equip de treball.** Això inclou formar els membres de l'entitat perquè aprenguin a reconèixer i evitar amenaces com el phishing i promoure bones pràctiques, com ara no obrir arxius adjunts sospitosos o enllaços desconeguts.

Amb aquests principis bàsics, les entitats poden començar a construir una base sòlida de seguretat digital que protegeixi tant la seva informació com la seva activitat diària.

Avaluació inicial

Abans d'implementar qualsevol mesura de ciberseguretat, és fonamental que l'entitat faci una avaluació inicial per entendre la seva situació actual i identificar les àrees de millora. Aquesta fase permet establir prioritats i garantir que els recursos es destinin a protegir els actius més crítics.

Diagnòstic de riscos

El primer pas és identificar quins són els principals riscos que poden afectar l'entitat. Això inclou:

- *Anàlisi de vulnerabilitats:* revisar els sistemes, xarxes i eines digitals per detectar punts febles que podrien ser aprofitats pels ciberdelinqüents.

- *Identificació de possibles amenaces.* considerar tant riscos externs (com atacs de phishing o malware) com interns (errors humans o mala configuració dels sistemes).
- *Avaluació de l'impacte potencial:* determinar quines serien les conseqüències si un risc es materialitzés, com ara la pèrdua de dades o la interrupció dels serveis.

Classificació de dades sensibles

No totes les dades que gestiona una entitat tenen el mateix nivell de sensibilitat. És important identificar quines dades requereixen un major nivell de protecció:

- *Dades personals:* informació de persones beneficiàries, donants, voluntariat o treballadors/es, que està protegida pel RGPD.
- *Dades financeres:* comptabilitat, transaccions i informació bancària de l'entitat.
- *Informació estratègica:* documents interns, plans estratègics o dades sobre projectes que, si es filtren, podrien comprometre l'activitat de l'entitat.

Un cop classificades les dades, es poden establir prioritats de protecció per a cadascun dels tipus identificats.

Estudi del nivell de maduresa digital

És essencial entendre el punt de partida de l'entitat en termes de seguretat digital. Per això, es poden utilitzar eines o qüestionaris per avaluar:

- *Infraestructura tecnològica:* està actualitzada i protegida amb mesures bàsiques com antivirus, tallafocs i còpies de seguretat?
- *Polítiques de seguretat:* l'entitat disposa de normes clares sobre l'ús de dispositius, gestió de contrasenyes o accés a dades?
- *Coneixement del personal:* els membres de l'equip estan formats per reconèixer i respondre a possibles amenaces cibernètiques?

Aquest estudi permet identificar fortaleses i febleses, així com establir un pla d'acció adaptat a les necessitats i capacitats específiques de l'entitat.

Resultats de l'avaluació

Un cop finalitzada l'avaluació, és recomanable resumir els resultats en un informe senzill que:

- Destaqui els riscos més urgents i les àrees vulnerables
- Proposi accions immediates per reduir els riscos detectats
- Defineixi prioritats per implementar mesures de ciberseguretat en funció dels recursos disponibles

Amb aquesta avaluació inicial, l'entitat estarà preparada per desenvolupar i aplicar una estratègia de ciberseguretat adaptada a la seva realitat.

Pla d'acció en ciberseguretat

Un cop completada l'avaluació inicial, és el moment de desenvolupar un pla d'acció estructurat que permeti a l'entitat millorar la seva ciberseguretat de manera progressiva i efectiva. Aquest pla ha de ser realista i adaptat als recursos disponibles, amb un enfocament clar en les prioritats identificades.

Creació d'un pla estructurat

El pla ha de començar amb una definició clara dels objectius i les responsabilitats dins de l'entitat:

- *Objectius específics:* què es vol aconseguir amb el pla? Per exemple, protegir dades personals, millorar la seguretat de les transaccions o prevenir atacs cibernètics.
- *Assignació de responsabilitats:* designar una persona o equip encarregat de liderar les accions de ciberseguretat. Si no hi ha personal tècnic, es pot buscar suport extern o col·laborar amb experts.
- *Establiment de terminis:* fixar un calendari realista per implementar les mesures previstes.

Mesures de protecció prioritàries

El pla d'acció ha d'incloure mesures concretes per millorar la seguretat digital de l'entitat. En primer lloc, és essencial treballar en la protecció de dades i sistemes. Això implica implantar sistemes d'encriptació per garantir la seguretat de les dades sensibles, configurar còpies de seguretat de manera periòdica i assegurar que s'emmagatzemin de forma segura, ja sigui fora de línia o al núvol. També cal implementar gestors de contrasenyes que assegurin que aquestes siguin robustes i segures.

En segon lloc, la gestió d'accés és un altre aspecte clau. Es recomana establir controls d'accés basats en rols (RBAC) per limitar qui pot accedir a dades o sistemes específics, reduint així la possibilitat de vulneracions. A més, incorporar l'autenticació multifactor (MFA) és una mesura molt efectiva per reforçar la seguretat dels accessos.

Finalment, la protecció de la xarxa és imprescindible per garantir la integritat de les comunicacions i els sistemes de l'entitat. Això es pot aconseguir mitjançant la instal·lació de tallafocs i sistemes antivirus en tots els dispositius.

També és recomanable utilitzar una VPN per assegurar les connexions remotes, especialment en entorns de teletreball o accés fora de les instal·lacions de l'entitat. Amb aquestes mesures, es poden mitigar gran part dels riscos digitals a què s'enfronten les entitats del tercer sector.

Gestió d'incidents de seguretat

Cap pla de ciberseguretat està complet sense una estratègia clara per gestionar incidents. Això inclou:

- *Definir un protocol de resposta:* crear procediments detallats per identificar, gestionar i resoldre incidents com atacs de phishing o pèrdua de dades.
- *Establir un punt de contacte:* designar una persona o equip responsable de coordinar la resposta davant incidents.
- *Comunicació interna i externa:* informar de manera clara i transparent els membres de l'entitat i, si escau, les persones afectades o les autoritats competents.

Formació i sensibilització

Un component essencial del pla és la formació contínua del personal:

- *Capacitació en bones pràctiques:* ensenyar com crear contrasenyes segures, identificar correus fraudulents i utilitzar eines de protecció.
- *Simulacions d'incidents:* realitzar exercicis pràctics per preparar l'equip davant situacions reals, com ara simulacions de phishing.

Seguiment i actualització del pla

La ciberseguretat és un procés en constant evolució, i el pla d'acció ha de ser revisat i ajustat periòdicament:

- *Monitoratge constant:* utilitzar eines per supervisar l'estat de la seguretat i detectar anomalies.
- *Auditories periòdiques:* realitzar revisions anuals per assegurar que les mesures implementades continuen sent efectives.
- *Actualització segons les necessitats:* Incorporar noves tecnologies o processos a mesura que apareguin noves amenaces o canvis normatius.

Amb un pla d'acció ben definit i una implementació progressiva, l'entitat estarà preparada per afrontar els reptes digitals i garantir la seguretat de les seves dades i operacions.

Compliment normatiu

El compliment normatiu és un aspecte essencial de la ciberseguretat.

Les entitats, que solen gestionar dades molt sensibles, tenen una gran responsabilitat a l'hora garantir que aquesta informació es protegeixi adequadament.

Les dades personals, financeres i de salut, entre d'altres, requereixen un tractament rigorós que compleixi amb les normatives legals vigents. Això no

només redueix els riscos de sancions econòmiques o legals, sinó que també reforça la credibilitat i la confiança en l'entitat.

Adoptar les mesures necessàries per al compliment normatiu no s'hauria de veure com una càrrega, sinó com una oportunitat per professionalitzar els processos de gestió de dades i per establir bones pràctiques que contribueixin al desenvolupament sostenible de l'entitat. Les normatives no només exigeixen un mínim de seguretat, sinó que també orienten cap a una gestió més eficient i ètica dels recursos digitals.

Normatives aplicables

Per garantir el compliment normatiu, és imprescindible conèixer les regulacions més rellevants aplicables a les entitats del tercer sector. Entre aquestes destaquen:

1. **Reglament General de Protecció de Dades (RGPD):** El RGPD és una normativa europea obligatòria per a totes les organitzacions que gestionen dades personals de ciutadans de la Unió Europea. Té com a objectiu principal protegir els drets i les llibertats de les persones pel que fa al tractament de les seves dades personals. Les entitats del tercer sector estan obligades a:
    - *Garantir la confidencialitat, integritat i disponibilitat de les dades*: això implica implementar mesures tècniques i organitzatives adequades, com l'encriptació, la gestió d'accés restringit i la formació del personal.
    - *Designar un Delegat de Protecció de Dades (DPD):* en els casos en què l'entitat tracti grans volums de dades sensibles, és obligatori comptar amb un DPD, responsable de supervisar el compliment de la normativa i actuar com a punt de contacte amb les autoritats.
    - *Notificar incidents de seguretat:* qualsevol violació de dades personals ha de ser comunicada a les autoritats competents en un termini màxim de 72 hores.

2. **Directiva NIS2:**

    Aquesta normativa europea se centra en la seguretat de les xarxes i la informació per millorar la resiliència cibernètica de les organitzacions.

    Tot i que inicialment estava pensada per a infraestructures crítiques, la seva aplicació s'ha ampliat a sectors com el tercer sector, especialment aquells que gestionen serveis essencials o dades d'alta sensibilitat. La directiva exigeix:

    - *Implementar controls de seguretat estrictes*: com l'avaluació periòdica de riscos, la protecció de sistemes crítics i la detecció de vulnerabilitats.
    - *Garantir la continuïtat dels serveis:* mitjançant plans de contingència i còpies de seguretat actualitzades.

- *Notificar incidents greus:* en cas d'atac, cal informar les autoritats de manera immediata per activar mecanismes de resposta coordinats.

3. **Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals (LOPDGDD):**
   Aquesta normativa espanyola complementa el RGPD, adaptant-lo al context nacional. A més d'establir requisits per al tractament de dades personals, inclou regulacions específiques sobre els drets digitals dels ciutadans. Alguns aspectes destacats són:
   - *Protecció especial de dades sensibles:* Les dades que tracten les entitats del tercer sector, com informació sobre menors, salut o ideologia, estan especialment protegides.
   - *Regulació de les transaccions digitals:* Assegura que les entitats compleixin amb els estàndards de seguretat en la captació de fons o la gestió de pagaments electrònics.
   - *Foment dels drets digitals:* La llei reconeix drets com el dret a la desconnexió digital, especialment important en entorns de treball híbrid o teletreball.

Aquestes normatives són una base imprescindible per establir bones pràctiques en la gestió de dades i sistemes digitals. El coneixement i aplicació d'aquestes regulacions no només protegeixen l'entitat de sancions, sinó que també contribueixen a una gestió més ètica i transparent.