Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Teletreball segur

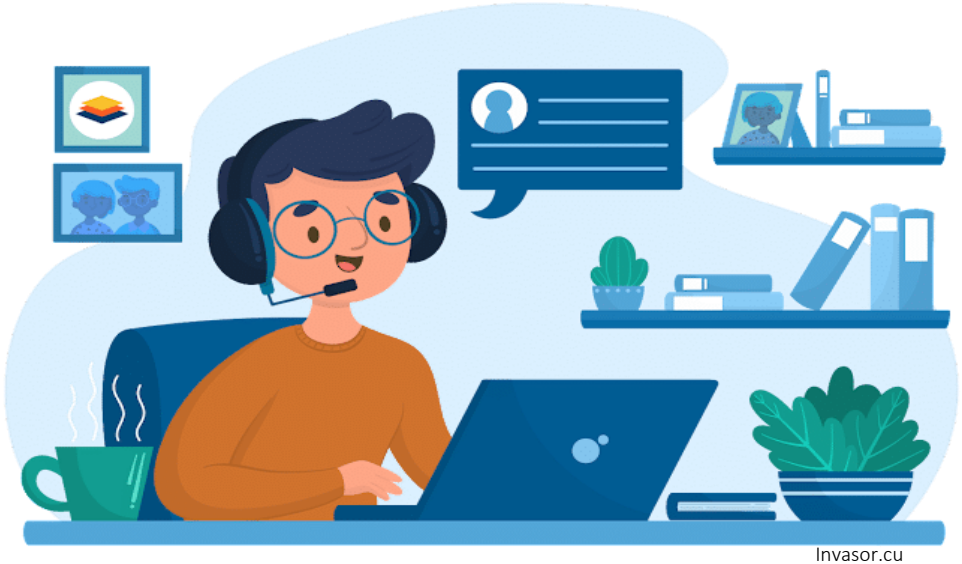
Conscienciació en ciberseguretat

Setembre de 2022

Imatge: Freepik.com

ÍNDEX

1. Treball i contextualització



Invasor.cu

El **desenvolupament de la tecnologia** i la tendència a viure en un món cada vegada més **globalitzat**, unit a **l'expansió empresarial** i a l'esclat del que ha estat un dels esdeveniments més importants produïts en les últimes dècades, la **pandèmia mundial provocada per la COVID-19**, ha accelerat l'aplicació d'un nou model empresarial basat en el **TELETREBALL** pel qual i, per suposat, fent ús de les eines corporatives, podem desenvolupar les nostres activitats professionals fora del nostre centre de treball ("**Home office**").

El teletreball s'imposa com una **modalitat flexible d'organització laboral** cada vegada més estesa en el món empresarial que implica que les empreses proporcionen als seus empleats un **accés remot a les seves infraestructures i serveis** per desenvolupar la seva feina fora de l'oficina. D'aquí, la importància ara mateix que l'accés remot a les infraestructures i eines corporatives sigui **segur** i que s'apliquin **mesures de seguretat i bones pràctiques** per evitar possibles riscos associats a aquesta modalitat de teletreball.

ÍNDEX

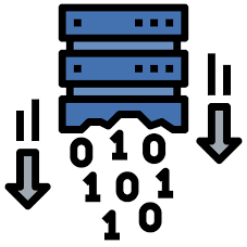
2. Teletreball i riscos associats

Ethic.es

Exposició a xarxes insegures

Compromís d'equips i dispositius

Pèrdua d'informació



Ús i equip dels dispositius corporatius

ÍNDEX

3. Teletreball i exposició a xarxes insegures

TIPUS D'ATACS QUE POTS PATIR SI ESTÀS TREBALLANT DES DE CASA

1. Atacs de tipus "Man in the middle".

L'atacant es posiciona enmig de la connexió i comunicacions entre el nostre dispositiu i el punt d'accés wifi. D'aquesta manera, pot tenir accés al trànsit generat i monitoritzar-nos, arribant a obtenir informació sobre l'activitat a la xarxa o fins i tot robar credencials d'accés.

2. Falses xarxes o xarxes fraudulentes

L'atacant crea una xarxa wifi copiant característiques (nom/SSID i pàgina d'inici) d'una xarxa legítima per, un cop connectats, i havent introduït les nostres credencials d'accés, obtenir el control dels nostres equips, monitoritzar-nos i aconseguir informació nostra.

El **teletreball** porta associat una connexió remota des de xarxes alienes a l'organització que no sempre podrà oferir les degudes garanties de seguretat, una major exposició a certes Ciberamenaces.

Revistaempresarial.com

CONSELLS PER QUAN ESTIGUIS TREBALLANT DES DE CASA

1. Assegura't de connectar-te a xarxes amb SSID conegut i en entorns de risc per exposició a llocs públics.
2. Restringeix l'accés a xarxes privades o inici de sessió en serveis web a xarxes configurades amb estàndards segurs (WPA2/WPA3).
3. Si la xarxa no ofereix garanties de seguretat optar per connectar-se a través de connexió 3G/4G/5G.
4. Utilitza sempre que sigui possible la connexió VPN de l'organització per garantir la confidencialitat.
5. Assegura't de navegar per pàgines web oficials amb xifrat HTTPS.
6. Deshabilita la connexió automàtica a xarxes wifi.

ÍNDEX

4. Teletreball i compromís d'equips i dispositius

1. Equips desprotegits i/o compromesos

- Equips personals: L'ús dels nostres dispositius personals en l'àmbit laboral (BYOD), és una eina útil, còmoda i àgil, ja que no hem de ser formats en el seu ús i la seva disponibilitat és total, però hem de tenir en compte que, quan anem a treballar amb informació corporativa, els nostres equips han de complir les configuracions i mesures de seguretat requerides.
- Equips corporatius: Quan treballem amb equips corporatius, hem de respectar les normes d'ús, així com assegurar-nos que es mantenen actualitzats (sistema operatiu i aplicacions) i que les mesures de seguretat estan actives i plenament funcionals. És recomanable la connexió periòdica a la xarxa corporativa per garantir-ne l'actualització i que es realitzin les revisions necessàries.

2. Infecció a través de xarxes o webs fraudulentes

Tenint en compte els riscos associats a l'exposició a xarxes insegures, els nostres equips poden ser infectats mitjançant malware en un punt d'accés a una xarxa wifi fals, així com al accedir a una web fraudulenta on el contingut de la qual conté codi maliciós que acabem descarregant en els nostres dispositius.

Per tant, què et recomanem al respecte?

- ✓ Mantingues actualitzat el teu sistema operatiu i les eines de seguretat (antimalware, firewall...) actives per prevenir atacs.
- ✓ Conècta't a la xarxa corporativa amb la freqüència recomanada pel Departament de sistemes.
- ✓ Tingues precaució amb els arxius adjunts en correus i descàrregues realitzades. Sempre descarregat la documentació de pàgines web oficials o programaris amb llicències.

ÍNDEX

Govern d'Andorra

5. Teletreball i pèrdua d'informació

ANC AD Agència Nacional de Ciberseguretat d'Andorra

La pèrdua d'informació sensible i confidencial d'una organització suposa un alt impacte i greus conseqüències econòmiques, reputacionals... etc. No només pel valor del coneixement associat, sinó també per l'afecció que pogués tenir en terceres parts (clients, proveïdors i usuaris en general), incompliments legals o contractuals, el dany a la imatge de la companyia, així com la conseqüent pèrdua de la confiança dipositada en aquesta pels seus clients.

Robatori o pèrdua de dispositius: Especialment sensible amb els equips portàtils i dispositius mòbils. Una persona que robi el nostre dispositiu, o bé se'l trobi perquè l'haguem perdut, tindrà accés potencial a informació i altres recursos personals i corporatius. Aquesta situació s'agreuja quan l'equip o dispositiu és d'un usuari administrador o amb alts privilegis.

Entorn de treball insegur: El teletreball implica, com el seu nom indica, exercir les nostres funcions de forma remota. Per tant, l'àmbit de treball determinarà la seguretat del desenvolupament de l'activitat. El treball des d'espais públics, més enllà de comportar connexions des de xarxes amb més risc, suposa una exposició a altres riscos físics com el "shouldersurfing" o robatori d'informació si no seguim les pautes de bloqueig de sessió o garantim la custòdia.

Malware o robatori de credencials: Bé per exposició a xarxes insegures, per una mala configuració i ús del navegador, per descarregar aplicacions i programari sense llicència o per no aplicar una política de contrasenyes i bloqueig de sessions, els ciberdelinqüents poden infectar els nostres equips amb objectius maliciosos diversos. En el moment que tinguin les nostres credencials o control del dispositiu, tindran accés a tota la informació i recursos d'acord amb els nostres privilegis assignats.

Emmagatzematge local: Quan treballem en remot podem tendir a treballar amb documentació en local per agilitat o dificultats en les connexions. Aquesta situació comporta una protecció inadequada de la informació si no és replicada a repositoris corporatius amb un control robust d'accés i garanties de disponibilitat (còpies de seguretat d'acord la política establerta).

Per tant, què et recomanem al respecte?

1. Utilitza contrasenyes robustes i, si és possible, un Doble Factor d'Autenticació / 2. Respecta sempre una Política de Pantalla i Escriptori nets / 3. Mantingues vigilats sempre els teus dispositius corporatius / 4. Mantingues actualitzats software i eines de seguretat /

5. Respecta la Política d'Emmagatzematge de la Informació, vetllant per allotjar-la en repositoris sobre els quals es realitzin còpies de seguretat.

ÍNDEX

6. Teletreball i l'ús indegut dels equips corporatius

L'usuari final és l'eslavó més important de la cadena i, al seu torn, és el més feble. Un empleat conscienciat amb la Seguretat de la Informació que es comporti i treballi conforme a les normes de seguretat establertes per l'organització és la gran base contra les amenaces, ja que els usuaris sempre són susceptibles de ser atacats pels ciberdelinqüents.

L'**ús indegut dels equips corporatius** és un **greu risc per la seguretat de la informació** i per als recursos tecnològics de la mateixa. Normalment, això ve associat a un **incompliment total o parcial de les normes d'ús** i a **comportaments inadequats** com els que passem a detallar:

- Oblidar o deixar desatesos equips o dispositius en llocs públics.
- No bloquejar la sessió de treball en els equips.
- Instal·lació d'aplicacions insegures per ús personal i que continguin malware.
- Instal·lació de programari sense llicència provinent de llocs no oficials.
- Ús de correu corporatiu per a ús personal.
- Navegació per llocs insegurs per ús no laboral.
- Canvis en la configuració per eliminar restriccions o obtenir més permisos dels assignats en les aplicacions.
- Desactivar eines o funcionalitats de seguretat.

Per tant, què et recomanem fer al respecte?

- ✓ Complirà les normes i polítiques establertes i vetllar pel seu compliment, notificant per això qualsevol NO conformitat que hagués estat detectada.
- ✓ Evitar les accions prohibides i indesitjades sobre els equips corporatius.
- ✓ Notificar els incidents de seguretat i situacions sospitoses, d'acord amb les instruccions facilitades per l'organització.
- ✓ Seguir les instruccions del personal de Sistemes per facilitar la gestió dels equips per part de l'organització.

ÍNDEX

7. Aïllament i teletreball solitari – Bones pràctiques

Per l'empresa

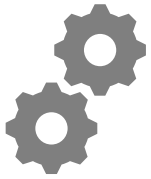
- ✓ L'empresa ha de facilitar una **cultura d'entorn de treball segur i col·laboratiu**.
- ✓ Ha d'establir **eines col·laboratives i canals de comunicació** entre treballadors per garantir el correcte treball en equip i evitar l'aïllament.
- ✓ Els responsables han de jugar un **paper de nexe de comunicació** i preocupar-se no només del bon acompliment del grup, sinó del **benestar propi dels empleats**.
- ✓ Assessorar els empleats amb **consells o bones pràctiques per un correcte acompliment** i resolució de problemàtiques habituals.

Per l'empleat

- ✓ Assimila la modalitat de treball abans de retroalimentar perspectives negatives. Per això, afavoreix la **recerca de solucions**.
- ✓ Mantenen **comunicació periòdica amb els companys** a través de les eines col·laboratives proporcionades per l'organització.
- ✓ Estableix una **rutina i realitza pauses periòdiques per moure't i relaxar-te**, per tal de mantenir un rendiment adequat. Continua sent important **cuidar la nostra salut amb activitat física habitual** i un control del nostre nivell d'estrès.
- ✓ Estigues **alerta dels riscos associats al teletreball** i informa't sobre les mesures de bon ús de la informació i equips corporatius.
- ✓ Notifica qualsevol **incidència de seguretat** i demana ajuda quan sigui necessari.

ÍNDEX

8. Teletreball i mesures que pot adoptar l'EMPRESA



- Mantenir un control de l'accés i ús dels dispositius i recursos per part del personal. Molt important gestionar els privilegis d'accés, d'acord amb el rol de l'empleat, aplicant per això el "Principi del mínim privilegi" i respectant, per això, els fluxos d'autorització i la retirada dels accessos als usuaris que causessin baixa.
- De la mateixa manera, s'ha de controlar la configuració dels sistemes, monitoritzant els canvis que puguin originar-se i que podrien comportar un risc per l'organització.
- Definir un mapa d'accessos per rol o perfil de l'usuari, així com controlar el programari permès/prohibit per a la seva descàrrega i instal·lació.

- Planificar la periodicitat de les còpies de seguretat per tal de garantir la integritat de la informació. Conscienciar l'usuari dels riscos associats a l'emmagatzematge d'informació en directori local.
- Implantar solucions tipus MDM (Mobile Device Managment) per un control i gestió robusta d'accessos, programari instal·lat, actualitzacions, xifrat de discos, esborrat remot de dades o còpies de seguretat periòdiques per dispositius mòbils corporatius i personals.
- La implantació d'una solució NAC permet implementar polítiques per al control d'accés de dispositius i usuaris.

- Les VPN o xarxes virtuals creen un túnel segur entre l'equip del treballador i la xarxa d'empresa. Amb aquesta solució, es facilita accés a la informació i als recursos TIC aplicant controls d'autenticació i xifrat que ajuden a garantir la confidencialitat i integritat de la informació.
- De la mateixa manera, és recomanable potenciar l'ús dels dispositius corporatius per garantir l'aplicació de les mesures de seguretat requerides, i, en cas d'oferir un accés des de dispositius aliens, garantir que estan protegits per les mesures de seguretat necessàries per mantenir la seguretat en tota la infraestructura corporativa.

- Les empreses han de vetllar per una adequada formació i conscienciació dels seus empleats sobre l'ús de la informació i sistemes i, en general, en l'àmbit de la Ciberseguretat. És molt important assegurar-se que tots els empleats siguin coneixedors dels principals potencials riscos o ciberamenaces que afecten el tractament de la informació interna i ús dels sistemes.
- D'igual manera, han de ser coneixedors del seu rol i responsabilitat en processos tan importants com la notificació i resposta davant incidents de seguretat.

- Confiar en professionals i especialistes en ciberseguretat per redactar, implementar o aplicar polítiques i procediments pel que fa a la seguretat de la informació, sempre que no es tinguin les eines necessàries.

ÍNDEX

9. Teletreball i mesures que pot adoptar l'USUARI

Mantenir actualitzat el **software** dels teus dispositius, així com l'eina **antivirus**.

Mantenir la informació en els **repositoris corporatius** i/o realitza **còpies de seguretat** periòdiques.

Entorn de treball segur: Assegura't de complir amb les normes de seguretat de la teva organització.

Evitar l'**aïllament derivat del teletreball**, mantenint una comunicació constant i fluida amb l'equip.

Utilitza **contrasenyes robustes** per usar els teus comptes en dispositius i, en la mesura del possible, **doble factor d'autenticació**.

En cas necessari i havent estat prèviament autoritzat, es **xifraran els suports extraïbles** com discs durs externs o pendrive i la informació enviada a través de canals insegurs.

Utilitza sempre el **VPN corporatiu**. Evita utilitzar **xarxes wifi públiques o insegures**. En el seu defecte, utilitza **xarxes mòbils 3G, 4G o 5G**.

Tingues precaució amb els **arxius adjunts i URLs incrustades** al correu electrònic. Presta atenció a **situacions sospitoses** en navegar, usar els equips i, en general, en interactuar amb terceres persones.

Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

ANDORRA
DIGITAL

Entitats col·laboradores

andorra
telecom

DAND
DIGITALAND
by Ibermática | TdA