Agència Nacional de Ciberseguretat d'Andorra

Conscienciació en ciberseguretat

Ús de tècniques criptogràfiques

Ús de tècniques criptogràfiques: Antecedents

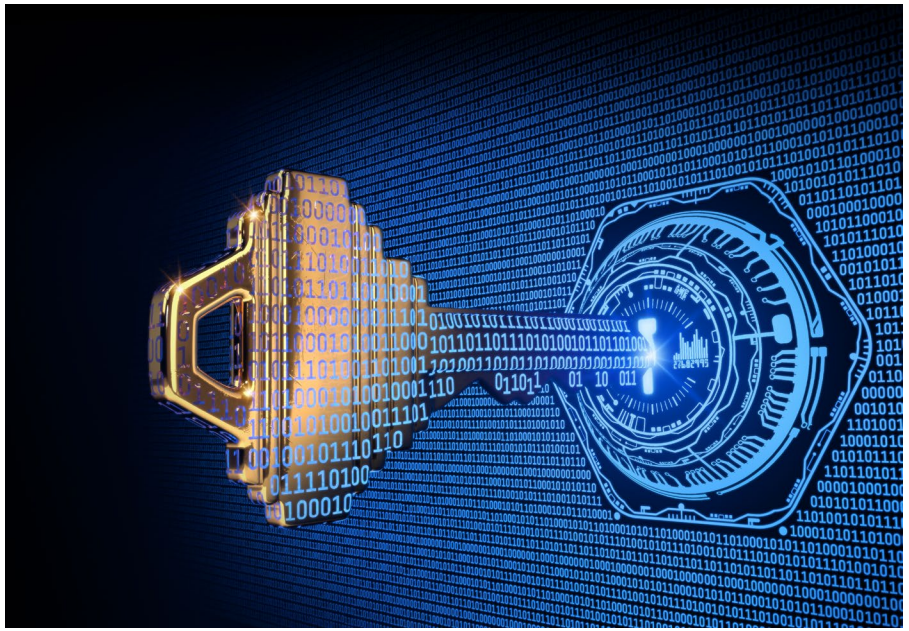
La informació sensible i confidencial que controlen a les organitzacions com ara les bases de dades, els registres d'usuaris, els correus electrònics que contenen informació privada, la informació subjecta a protecció legal, les còpies de seguretat, la informació emmagatzemada en dispositius extraïbles i mòbils... per la seva transcendència i importància pel negoci de les organitzacions, ha d'estar especialment protegida, tant en el trànsit de la informació, com durant el seu emmagatzematge.

Per protegir aquesta informació, a més de controlar l'accés a la mateixa i protegir els Sistemes d'Informació on es desa, és recomanable que s'utilitzin tècniques i eines criptogràfiques que xifrin les dades de l'organització, fent-les il·legibles per part d'aquells usuaris que no disposen de la clau de xifratge.

Ús de tècniques criptogràfiques: Antecedents

D'altra banda, les tècniques criptogràfiques també permeten signar digitalment els documents i els correus electrònics rellevants, garantint l'autenticitat del seu contingut i al no refús d'aquests.

Tant pel xifratge de la informació com per a l'ús de la firma digital, s'hauria d'elaborar una anàlisi prèvia que determinés quines dades de l'organització haurien de ser xifrades i quins usuaris requereixen tenir una firma digital. A més, es recomana l'ús de protocols segurs en les comunicacions, tant pels usuaris de l'organització com pels usuaris dels serveis oferts per part de l'organització (per exemple, l'ús d'una VPN per l'accés a la xarxa interna de l'organització per part dels seus empleats).



Ús de tècniques criptogràfiques: Objectius

L'objectiu de l'ús de tècniques criptogràfiques és assegurar la confidencialitat, integritat, disponibilitat i a no refusar la informació delicada controlada per les organitzacions, tant la informació que s'emmagatzema com la informació que es troba en trànsit com per exemple: dades de caràcter personal, informació sensible o confidencial, còpies de seguretat al núvol o en proveïdors externs, dades en dispositius mòbils o dispositius extraïbles, contractes, factures i intercanvis comercials o amb les administracions públiques, accessos remots, etc.

Per això, recomanem a les organitzacions que realitzin una llista d'elements a tenir en compte i vagin revisant que es compleixen una sèrie de controls, amb l'objectiu de verificar el compliment de la Política de Seguretat de la Informació de la mateixa pel que fa a l'ús de tècniques criptogràfiques.

Ús de tècniques criptogràfiques: Tipus de controls criptogràfics

Quins controls s'haurien de tenir en compte en l'àmbit criptogràfic dins una entitat?

Controls
Informació susceptible de ser xifrada: Identificar la informació de la vostra empresa que s'hauria de xifrar.
Ús de la firma electrònica: Implantar l'ús de la firma electrònica en els intercanvis comercials i amb la administració electrònica.
Certificats web: Adquisició d'un certificat web per la pàgina web o botiga electrònica.
Xifratge de dades delicades en contractar serveis externs: Comprovar que s'emprin canals i eines de xifratge per les comunicacions i tractament de la informació en el moment de contractar serveis.
Xifratge de dades sensibles quan es sol·licita desenvolupar una aplicació: Comprovar que es xifren les credencials d'accés quan es sol·licita el desenvolupament d'una web o d'aplicacions que impliqui l'inici de sessió.
Accés des de l'exterior amb una VPN: Autoritzar l'accés des de l'exterior al personal que no necessiti establir canals VPN xifrats.
Algorismes de xifratge autoritzats: Aplicació i revisió d'algorismes de xifratge adequats pels sistemes.
Aplicacions autoritzades per usos criptogràfics: Disposar d'un llistat d'aplicacions autoritzades pel xifratge.
Ús de protocols segurs de comunicació: Implementar protocols segurs per accedir a espais administratius, de transferències de fitxers, a servidors tant si estan en les instal·lacions de la mateixa entitat com si estan en algun proveïdor.
Xifratge de la xarxa WI-FI de l'organització: Configurar la xarxa WI-FI de l'entitat amb el xifratge estandarditzat més segur, actualment és el WPA2.

Ús de tècniques criptogràfiques: Política de criptografia

1. Informació susceptible de ser xifrada: La classificació de la informació ha de servir per saber quina ha de ser xifrada i quina no. Això, amb la finalitat de garantir-ne la confidencialitat i la integritat. Les dades a tenir en consideració perquè siguin protegides són:
Informació delicada de caràcter personal o confidencial, els registres amb les credencials d'autenticació, la informació emmagatzemada en dispositius personals o de tercers que manquen dels controls de seguretat adequats, la informació transferida a través de xarxes de telecomunicació no fiables o en suports d'emmagatzematge físics i que no han estat protegits adequadament.

2. Ús de la firma electrònica: Farem ús de la signatura electrònica només en aquells casos en què sigui imprescindible, amb l'objectiu de garantir l'autenticitat i a no refusar la informació, per exemple, en realitzar tràmits amb les administracions públiques.

3. Certificats web: Per garantir la seguretat de la informació en els llocs web, en especial, si es tracta d'una botiga en línia.

4. Accés des de l'exterior mitjançant una VPN: Si es té treballadors fent teletreball o s'autoritza l'accés des de l'exterior als servidors de les instal·lacions, s'haurà d'habilitar canals de VPN que estiguin degudament xifrats i que garanteixin la confidencialitat i integritat de les comunicacions.

Ús de tècniques criptogràfiques: Política de criptografia

5. Xifratge de dades delicades quan es contracten serveis externs: Si és necessari contractar serveis externs que tractin dades confidencials o sensibles, s'ha de verificar que les transferències de dades són segures, xifrant les dades abans de transferir-les o utilitzant canals segurs.

6. Aplicacions autoritzades per usos criptogràfics: Convé tenir una llista de les aplicacions autoritzades per fins criptogràfics i detallar l'ús concret que se'n fa d'aquestes.

7. Ús de protocols segurs de comunicació: Caldrà facilitar als empleats de l'organització formació i eines de comunicació que utilitzin protocols criptogràfics actualitzats. D'aquesta manera, es pot garantir la confidencialitat de la informació en el moment d'accedir als Sistemes d'Informació de l'organització.

8. Xifrat de la xarxa WI-FI de l'entitat: Configurar la xarxa Wi-Fi de l'organització amb l'estàndard de xifrat més segur (actualment és el WPA2) i després canviar la clau d'accés que apareix per defecte.

9. Algorismes de xifratge autoritzats: Per evitar l'ús de sistemes de xifratge obsolets, és aconsellable aplicar algorismes de xifratge actuals comprovant que estiguin vigents. D'altra banda, s'aconsella l'ús de sistemes de xifratge asimètric, en detriment dels sistemes de xifratge simètric.