SGSI-P-5.1.1
Política de Seguretat de la Informació

Data de revisió: 22/12/2023

ÍNDEX

1. DEFINICIÓ DE SEGURETAT DE LA INFORMACIÓ.

La informació suposa per Andorra Telecom (AT en endavant) un actiu molt valuós i crític sense el qual la Companyia no podria desenvolupar la seva activitat. Per aconseguir una adequada gestió d'aquest actiu, AT utilitza la informació de manera exacta, integra i garantint la seva disponibilitat.

La seguretat de la informació es defineix com la protecció de la informació davant un ampli conjunt d'amenaces per assegurar la continuïtat del negoci, minimitzar els riscs i maximitzar el retorn sobre les inversions i oportunitats.

Per això, es reconeix la importància de les mesures de seguretat que garanteixin que la informació no sigui afectada per amenaces, internes i externes, com poden ser: errors humans, accions malintencionades (fraus, malversacions, sabotatges, violacions de la intimitat...), errors tècnics i amenaces de força major com els desastres naturals.

La Direcció de AT té la responsabilitat de desenvolupar les directives de seguretat. L'adopció d'aquestes per part de la Companyia, permetrà minimitzar els riscos potencials als quals es troba exposada en el desenvolupament de les activitats de negoci.

2. ABAST DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ.

La Política de Seguretat de la Informació és aplicable a tota persona o software que tingui o pugui tenir accés a la informació de AT, ja sigui directament o mitjançant algun sistema d'informació, durant el desenvolupament de les seves funcions.

Per tant, els àmbits d'aplicació de la Política de Seguretat de la Informació són:

- Tots els treballadors de AT siguin o no empleats indefinits, incloent qualsevol persona aliena a AT que tingui accés a la informació gestionada o propietat de la mateixa així com qualsevol software que també hi tingui accés.
- A tota la informació i als sistemes d'informació propietat de AT o gestionats per la mateixa.

3. OBJECTIUS.

La Política de Seguretat de la Informació estableix les directives per a la formulació de normatives de seguretat, amb l'objectiu de salvaguardar i garantir els principis bàsics de la seguretat de la informació: confidencialitat, integritat, disponibilitat i traçabilitat.

Per a l'elaboració d'aquest document i la consecució dels objectius fixats s'han adoptat els següents aspectes clau:

- La informació de la Companyia i els seus sistemes d'informació són actius crítics, i per tant, han de ser protegits i s'ha d'assegurar la seva disponibilitat.
- La informació de AT ha de ser protegida segons els seus requisits legals, valor, cripticitat i sensibilitat.

- La responsabilitat de protegir aquests actius recau sobre tots els empleats i col·laboradors externs que tenen accés a la informació.
- Les mesures de seguretat aplicades a la informació s'han d'establir tenint en compte la seva classificació, que determinarà el seu nivell de confidencialitat, integritat, disponibilitat i traçabilitat. Aquestes han de determinar-se conforme a una avaluació contínua del risc.

4. DECLARACIÓ DE PRINCIPIS.

Els principis de seguretat de la informació sobre els que s'elaboren les Normatives de Seguretat de la Informació són els següents:

- La informació és protegida durant tot el seu cicle de vida, des de la seva creació o recepció fins al seu processament, comunicació, transport, emmagatzematge, difusió a tercers i la seva eventual destrucció.
- AT protegeix la informació contra accessos no autoritzats, la difusió indeguda o la pèrdua de la mateixa.
- Cada empleat té l'obligació i el deure de protegir adequadament la informació conforme a les normatives de seguretat.
- Tot el personal, incloent el personal extern o terceres parts amb accés a la informació de AT, estan sotmesos a les normatives de seguretat de AT.

5. CONSIDERACIONS DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ.

- La Política de Seguretat de la Informació, ha estat aprovada per la Direcció General de AT.
- El seu contingut, junt amb les Normatives de Seguretat de la Informació, és de compliment obligat per tot el personal de AT i els externs contractats.
- El compliment de la Política de Seguretat de la Informació és necessari per la protecció dels drets legals de AT. Qualsevol persona que la incompleixi estarà subjecte a les mesures disciplinàries i legals que consideri la Direcció de AT.
- La Política de Seguretat de la Informació és un document viu que s'ha d'actualitzar i modificar sempre que sigui necessari.
- La Direcció de AT promourà les accions necessàries per a què el personal de AT, el personal extern i els tercers coneguin i apliquin tots els aspectes inclosos en aquesta política.

6. ESFORÇOS DE SEGURETAT COMPARTITS PER TOTS.

La Direcció de AT ha establert un Comitè de Risc, format per una sèrie de membres preestablerts, que es reuniran de forma periòdica per tractar els temes rellevants en matèria de seguretat.

El Comitè de Risc s'encarregarà de la revisió i aprovació de les Normatives de Seguretat de la Informació i de mantenir-les actualitzades davant canvis significatius. Al mateix temps, serà

responsabilitat del Comitè de Risc l'aprovació de les iniciatives necessàries per millorar la seguretat de la informació així com de promoure la conscienciació i implicació de tots els empleats. D'aquesta manera, s'assegura que qualsevol acció en matèria de seguretat serà adoptada per tota l'organització.

7. NORMATIVES DE SEGURETAT DE LA INFORMACIÓ.

Per assolir els objectius i principis inclosos en aquesta política, s'han desenvolupat una sèrie de normatives, les quals articulen les regles generals de seguretat de la informació i s'agrupen d'acord a dominis establerts.

Aquestes normatives constitueixen una base pel desenvolupament de mesures de seguretat específiques, que es concreten mitjançant la formalització de procediments.

Les normatives han estat definides d'acord amb l'estàndard ISO 27001:2013 que estableix un marc de referència de seguretat reconegut internacionalment. Els requeriments de seguretat establerts per la ISO 27001:2013 es defineixen mitjançant objectius de control que s'agrupen segons els dominis següents:

- **Domini 6. Organització de la seguretat d'informació.** Definició dels rols de la direcció i empleats de AT, així com els aspectes organitzatius i les responsabilitats per mantenir la seguretat de la informació.
- **Domini 7. Seguretat en els recursos humans.** La seguretat del personal, amb la finalitat de definir i implementar les funcions i responsabilitats en els llocs de treball.
- **Domini 8. Control d'actius.** Inventari, manteniment i classificació d'actius de tota la organització, incloent la informació, amb la finalitat de mantenir un nivell de protecció adequat.
- **Domini 9. Control d'accés lògic.** Control d'accés lògic per a protegir els actius d'informació de AT, prevenint accessos innecessaris o no autoritzats.
- **Domini 10. Controls criptogràfics.** Gestió i control dels sistemes criptogràfics.
- **Domini 11. Seguretat física i ambiental.** La seguretat física i de l'entorn amb la finalitat de controlar l'accés a la informació de caràcter sensible.
- **Domini 12. Gestió d'operacions.** Gestió i control de les operacions, tant de xarxes externes com internes de AT.
- **Domini 13. Seguretat en les comunicacions.** Gestió i control de comunicacions, tant de xarxes externes com internes de AT.
- **Domini 14. Adquisició, desenvolupament i manteniment dels sistemes d'informació.** Definició de requisits de seguretat de desenvolupament i manteniment de sistemes de la informació, amb l'objectiu de garantir en tot moment el correcte funcionament dels recursos informàtics. S'inclou l'elaboració de plans preventius davant possibles desastres així com procediments de recuperació de dades i informació crítica de AT.
- **Domini 15. Relacions amb els proveïdors.** Gestió i control de les relacions amb els proveïdors així com els serveis prestats per tercers **Domini 8. Seguretat en els recursos**

humans. La seguretat del personal, amb la finalitat de definir i implementar les funcions i responsabilitats en els llocs de treball.

- **Domini 16. Administració dels incidents de seguretat**. Gestió, comunicació i resposta davant incidències de seguretat.
- **Domini 17. Administració de la continuïtat del negoci**. Continuïtat de negoci per garantir el restabliment dels processos crítics de negoci en cas d'interrupció d'aquests.
- **Domini 18. Compliment.** Identificació de la legislació andorrana vigent aplicable per assegurar el seu compliment, i comprovacions periòdiques per validar l'adequació a les normes de seguretat de l'organització.

8. RESULTATS ESPERATS.

Els resultats esperats de la Política de Seguretat són els següents:

- Millora de la gestió de la seguretat sobre una base contínua. L'organització disposarà de millors recursos de seguretat en forma de coneixements, procediments i eines.
- Consolidar la confiança en la Companyia per part de clients i proveïdors, acompanyada d'una millora en la imatge pública.
- Disminució de costos derivats d'incidents de seguretat, mitjançant la progressiva implantació de controls de seguretat.
- Assegurament del compliment dels requisits legals i ètics.

GLOSSARI

Actiu: Qualsevol cosa que pot tenir valor per la Companyia, poden esser dels tipus informació, programari, físics, serveis, persones o intangibles.

Amenaça: Causa potencial d'un incident no desitjat, el qual pot resultar en un impacte a un sistema o organització.

Confidencialitat: Característica que assegura que una informació privada o confidencial no es comunica a persones no autoritzades, durant el seu emmagatzematge, tractament o transit.

Continuïtat de Negoci: Temps tolerable que pot estar un procés de negoci interromput sense provocar un impacte elevat a la Companyia.

Criticitat: Importància d'un actiu en funció del dany que es produiria a la Companyia en cas de que es materialitzes una amenaça sobre aquest.

Dades de Caràcter Personal: Qualsevol informació referent a persones físiques identificades o identificables.

Disponibilitat: Característica que assegura que els sistemes funcionin puntualment i que els serveis no siguin denegat als usuaris autoritzats.

Impacte: Conseqüència sobre un actiu de la materialització d'una amenaça.

Incident de Seguretat: Esdeveniment identificat en un sistema, servei o xarxa que indica una possible escletxa en la política de seguretat o una fallida en els salvaguardes, o prèviament una situació no coneguda que pot ser rellevant en matèria de seguretat.

Integritat: Característica que prevé contra la modificació o destrucció no autoritzades d'actius del domini.

ISO: *International Organitzation for Standarization* és una organització internacional no governamental que produeix normes reconegudes internacionalment industrials i comercials.

Normatives de Seguretat: Conjunt de normes que suporten els objectius recollits en la Política de Seguretat de la Informació.

Política de Seguretat de la Informació: Declaració d'alt nivell dels objectius, directrius i compromís de la Companyia per aconseguir la gestió de la seguretat.

Procediments: Instruccions de treball que conformen tasques i activitats específiques d'operativa diària.

Risc: Probabilitat de que es materialitzi una amenaça, produint un impacte determinat en un actiu, domini o en tota la Companyia.

Traçabilitat: Característica que permet la reconstrucció, la revisió i la examinació de una seqüència de esdeveniments.

Tercera Part: Persona o entitat reconeguda com a independent per les parts participants, relacionades en la situació en qüestió.