Acords

Acord de l'11-12-2024 del Consell Superior de la Justícia d'aprovació del Reglament d'ús acceptable dels actius de la informació.

Exposició de motius

El Consell Superior de la Justícia facilita als usuaris del Consell i de l'Administració de justícia la utilització d'uns determinats mitjans tècnics que garanteixen la rapidesa i l'eficàcia en la prestació dels serveis que tenen assignats. Entre aquests instruments propietat del Consell Superior de la Justícia, destaquen principalment els equips informàtics i els de comunicació per la seva aplicació massiva i el rol preponderant que han adquirit.

L'ús inadequat dels sistemes d'informació exposa el Consell Superior de la Justícia i l'Administració de justícia a riscos cibernètics, inclosos atacs de virus i de programari de segrest, compromís de sistemes i serveis de xarxa o violació de dades, entre altres. Per a la protecció dels actius d'informació, es fa necessària la regulació d'unes pautes de conducta amb la finalitat de garantir-ne el bon ús.

Igualment, es pretén conscienciar tots els usuaris dels actius d'informació (en endavant, "l'usuari") dels avantatges que comporta la bona utilització de les eines que se'ls facilita, tant per la millora en la distribució dels recursos materials de què es disposa, com per la incidència en matèria de seguretat que suposa en totes les àrees de treball, sense oblidar l'increment d'eficiència i qualitat en la prestació del servei als ciutadans.

En efecte, d'una banda, l'usuari ha de conèixer els riscos no tecnològics, com podrien ser la informació en paper a l'abast de persones no autoritzades, la falta de confidencialitat dels mitjans de comunicació tradicionals, el perill de sostracció o pèrdua dels dispositius o l'accés físic de terceres persones a les zones de treball.

D'altra banda, en molts llocs de treball es té accés a ordinadors, dispositius mòbils i portàtils amb connexió a la xarxa i a l'exterior (Internet). Són, doncs, una porta d'entrada als seus recursos d'informació. És essencial preparar els usuaris per evitar incidents que puguin iniciar-se en el seu lloc de treball: accessos no autoritzats als ordinadors i des d'ells a aplicacions; infeccions per codi maliciós; sostracció i fuita de dades en format digital; atacs d'enginyeria social, és a dir, enganys per manipular la víctima per obtenir informació confidencial com credencials o aconseguir que faci alguna acció per ell com instal·lar un programa, enviar correus o fer algun ingrés.

Per garantir un ús adequat dels dispositius i mitjans de l'entorn de treball, i minimitzar l'impacte que tots aquests riscos poden tenir, el Consell Superior de la Justícia ha considerat oportú aprovar el Reglament d'ús acceptable dels actius de la informació, document que pretén informar els usuaris de les normes d'ús dels mitjans tecnològics a la seva disposició, establint determinades pràctiques com a prohibides i alhora advertint els usuaris des de les mesures de control per part del Consell amb aquesta finalitat i de les conseqüències i responsabilitats en què es pot incórrer derivades de l'ús inadequat d'aquests actius.

D'acord amb aquestes consideracions, el Consell Superior de la Justícia, a proposta del Comitè de Seguretat de la Informació, en la sessió de l'11 de desembre del 2024, acorda el següent:

Article únic

S'aprova el Reglament d'ús acceptable dels actius de la informació, que entrarà en vigor l'endemà de publicar-se al *Butlletí Oficial del Principat d'Andorra*.

Dipòsit legal: AND.2-2015

Reglament d'ús acceptable dels actius de la informació

Article 1. *Objecte*
Aquest Reglament té per objecte establir l'ús acceptable d'equips informàtics i altres dispositius electrònics mitjançant la regulació de l'ús dels mitjans tècnics, els informàtics i les eines de comunicació, així com establir els protocols per fer les comprovacions que s'estimin necessàries si es detecta un abús o un ús inadequat en la utilització d'aquestes eines.

Article 2. *Àmbit d'aplicació*
Aquesta normativa s'aplica a l'ús per part dels usuaris, tan interns com externs, dels recursos d'informació, electrònics i informàtics i de la xarxa per interactuar amb xarxes internes i sistemes, siguin de propietat o estiguin a disposició del Consell Superior de la Justícia o de l'Administració de justícia per qualsevol altre títol.

Article 3. *Compliment*
1. El Comitè de Seguretat de la Informació (CSI) verifica el compliment d'aquesta normativa mitjançant diversos mètodes, inclosos, entre d'altres, auditories internes i externes i indicadors per verificar-ne el compliment.

2. Qualsevol excepció a aquesta normativa ha de ser aprovada pel Consell Superior de la Justícia de forma prèvia.

Article 4. *Comunicació d'incidències de seguretat*
1. En cas d'incident de seguretat o de sospita d'incident, l'usuari ho ha de notificar immediatament a l'Àrea de Transformació Digital mitjançant el correu electrònic prèviament notificat al personal.

2. Igualment, els usuaris han de comunicar a l'Àrea de Transformació Digital qualsevol deficiència que detectin en matèria de seguretat, així com qualsevol millora que considerin oportuna per garantir-la.

Article 5. *L'ús general*
1. Els recursos a disposició dels usuaris que presten servei al Consell Superior de la Justícia o a l'Administració de la justícia, així com l'accés a determinats recursos informàtics que faciliten el desenvolupament del seu treball, han de ser utilitzats per a les tasques pròpies, d'acord amb les funcions que tenen assignades.

2. En compliment del Sistema de gestió de la seguretat de la informació (SGSI), s'estableixen les mesures de seguretat oportunes per a la protecció dels recursos informàtics. L'usuari que hi té accés ha de ser responsable de la seva custòdia, protegint-los davant d'amenaces com ara accessos no autoritzats, ús indegut, errors o sostraccions, entre altres.

3. El programari, els arxius, el correu electrònic i altres documents informàtics instal·lats o continguts en la xarxa, així com qualsevol eina informàtica, han de ser utilitzats amb una finalitat professional.

4. Per evitar comprometre les mesures de seguretat establertes, llevat que es disposi d'una autorització expressa i per escrit del CSI, no es poden dur a terme les pràctiques següents:

a) Destruir, alterar, inutilitzar o danyar de qualsevol altra forma els recursos informàtics, programes, dades, suports i documents.

b) Intentar desxifrar les claus, sistemes o algorismes de xifratge i qualsevol altre element de seguretat establert.

c) Modificar o desactivar els mecanismes de seguretat implantats per a la protecció dels recursos informàtics i dels sistemes d'informació.

d) Accedir a informació que no sigui necessària per al desenvolupament de les funcions de cada persona.

e) Deixar els recursos de tractament d'informació desatesos sense les mesures de bloqueig adequades o tenir suports amb informació sensible en llocs poc segurs.

Dipòsit legal: AND.2-2015

Article 6. *L'ús de la informació*
1. La informació que s'ha generat en el marc d'una relació contractual o laboral amb el Consell Superior de la Justícia o l'Administració de justícia, emmagatzemada en dispositius electrònics i informàtics, sigui de propietat o d'acord amb qualsevol altre títol del Consell Superior de la Justícia o de l'Administració de justícia, dels usuaris o d'un tercer, és propietat exclusiva del Consell Superior de la Justícia o l'Administració de justícia en funció de l'àmbit que s'escaigui en cada cas.

2. La informació confidencial o amb dades de caràcter personal, ja es trobi en dispositius d'emmagatzematge o en documentació o informació visible a la pantalla de l'ordinador, ha de ser protegida d'accessos no autoritzats.

3. No s'ha de mantenir la informació en llocs a la vista sense el control degut de la persona responsable.

4. Addicionalment i en la mesura que sigui possible, les pantalles s'han d'orientar de manera que es redueixi al màxim l'angle de visió dels usuaris no autoritzats.

Article 7. *Les activitats no acceptades*
Es consideren prohibides les activitats següents:

1. La còpia no autoritzada de material protegit per drets d'autor, incloent-hi, entre d'altres, la digitalització i la distribució de fotografies de revistes, llibres o altres fonts, música i la instal·lació de qualsevol programari per al qual no es tingui una llicència activa.

2. L'exportació de programari, d'informació tècnica o de tecnologia de xifratge.

3. L'escaneig de ports o l'escaneig de seguretat, llevat que l'autoritzi prèviament el CSI.

4. La interferència o la denegació del servei a qualsevol usuari.

5. La utilització de qualsevol programa, l'ordre, el conjunt d'ordres o l'enviament de missatges de qualsevol tipus amb la intenció d'interferir o inhabilitar la sessió terminal d'un usuari, per qualsevol mitjà, localment o a través d'Internet, Intranet o Extranet.

6. Altres activitats que estableixi prèviament el CSJ a proposta del CSI en el marc del Sistema de gestió de seguretat de la informació (SGSI).

Article 8. *La utilització dels equips informàtics*
1. Els equips informàtics facilitats als usuaris són propietat del Consell Superior de la Justícia i de l'Administració de justícia, que els posa a la seva disposició per al desenvolupament de la seva activitat professional.

2. Queda prohibit alterar els equips informàtics o connectar-ne d'altres sense comptar amb l'autorització expressa de l'Àrea de Transformació Digital (ATD).

Article 9. *La utilització dels programes*
1. En qualsevol cas, la informació de caràcter confidencial inclosa en els arxius i documents propietat del Consell Superior de la Justícia o l'Administració de justícia no pot enviar-se mitjançant cap tipus d'eina a terceres persones físiques o jurídiques sense l'autorització expressa del superior jeràrquic o per mandat judicial, i en qualsevol cas complint el que disposa la normativa reguladora de la Llei qualificada de protecció de dades personals.

2. Està prohibida la utilització, la còpia o la reproducció dels programes informàtics instal·lats en els equipaments de treball per a fins aliens a l'activitat professional.

3. Davant el risc que arxius o programes procedents de fonts no conegudes continguin virus, queda prohibit executar arxius procedents de fonts no conegudes sense l'autorització expressa del superior jeràrquic i del CSI.

Dipòsit legal: AND.2-2015

Article 10. *Les mesures de seguretat en l'accés lògic*

1. El control d'accés als sistemes d'informació està basat en l'ús de credencials que estan lligades a perfils d'accés. Aquests perfils han estat establerts d'acord amb les funcions que exerceix cada usuari.

2. Per a l'accés als sistemes del Consell Superior de la Justícia i l'Administració de justícia, s'empra un sistema d'autenticació per diferents factors. La vinculació amb aquestes entitats comporta l'acceptació de la utilització d'aquest sistema.

3. L'identificador d'usuari, així com la corresponent contrasenya i el multifactor d'autenticació, són confidencials, personals i intransferibles. És responsabilitat de l'usuari l'ús que se'n faci.

4. Cada usuari ha de vetllar per la confidencialitat de la seva contrasenya i en cap cas no ha de mantenir-la en arxius digitals, paper o qualsevol altre tipus de suport de forma llegible o accessible. No es pot comunicar a una altra persona l'identificador d'usuari i contrasenya, ni utilitzar una sessió oberta amb una altra identitat.

5. Si l'usuari té la sospita que la seva contrasenya ha estat coneguda de forma fortuïta o fraudulentament per persones no autoritzades, ha de modificar-la i notificar la incidència mitjançant el correu electrònic prèviament notificat al personal.

Article 11. *L'ús del certificat digital*

1. Els certificats digitals autoritzats per al desenvolupament de les funcions encomanades són els certificats professionals autoritzats per la Comissió Nacional d'Acreditació de Serveis de Confiança (CNAC), vàlids per a la signatura o el xifratge de documents i correus electrònics, l'autenticació en sistemes d'informació i la realització de tràmits amb plenes garanties jurídiques i tècniques.

2. En el cas de la signatura electrònica, el certificat digital s'ha d'utilitzar quan els usuaris hagin d'acreditar la seva pertinença al Consell Superior de la Justícia o a l'Administració de justícia.

3. Els certificats es poden revocar sense avís previ i les claus de xifratge es poden recuperar eventualment quan hi hagi una causa justificada i legítima, que faci necessari l'accés al contingut del correu corporatiu o desxifrar informació ubicada a les estacions de treball, als servidors de xarxa o als serveis al núvol. En cap cas no es podrà recuperar la clau d'identificació i signatura electrònica.

4. L'ús dels certificats s'ha de fer d'acord amb el que s'estipuli al Sistema de gestió de seguretat de la informació (SGSI).

Article 12. *L'ús de la xarxa*

1. La navegació per la xarxa d'Internet es fa amb finalitats professionals.

2. Els usuaris són els únics responsables de les sessions iniciades a Internet amb els equips informàtics que tenen a la seva disposició.

3. Es reserva el dret a filtrar el contingut al qual pot accedir l'usuari mitjançant Internet des dels equips informàtics, així com a registrar els accessos fets des d'aquests equips.

4. Es consideren prohibides les activitats següents:

a) L'accés a les xarxes socials d'Internet, exceptuant els serveis que per les seves característiques estiguin autoritzats a accedir-hi.

b) La utilització de programes P2P o similars, de xats o de programes de conversa en temps real no autoritzats pel CSI.

c) La modificació de les configuracions dels navegadors dels equips informàtics.

d) L'accés, el buidatge i l'emmagatzematge de pàgines amb continguts il·legals, exceptuant els serveis que per les seves pròpies característiques estiguin autoritzats a accedir-hi.

5. En l'ús necessari d'Internet per a la realització de les tasques professionals, els usuaris han de ser conscients que en l'exercici de les seves funcions representen el Consell Superior de la Justícia o l'Administració de justícia i, per tant, es comprometen en la seva conducta a reflectir l'ètica, la professionalitat, la cortesia i la responsabilitat corresponent.

Dipòsit legal: AND.2-2015

Article 13. *El correu electrònic i les activitats de comunicació*

1. De forma general s'han de seguir les indicacions següents:

a) El correu electrònic és exclusivament per a ús professional, ja que és una eina de treball. Qualsevol ús particular ha de ser puntual i limitat.

b) El Consell Superior de la Justícia o l'Administració de la justícia, com a responsables i gestors del correu electrònic, poden prendre les mesures necessàries en el marc de les seves competències quan observin indicis d'un ús indegut per part d'un usuari.

c) En el cas que es rebi un missatge erroni identificat tant pel contingut com pels remitents, s'ha d'eliminar.

d) Les comunicacions efectuades en el desenvolupament de les tasques professionals en cap cas no s'han d'enviar des de comptes personals.

e) Quan s'enviïn correus electrònics a múltiples destinataris els quals no es coneixen entre si, s'han d'enviar sempre amb còpia oculta per no difondre les adreces sense el consentiment degut.

f) Abans d'obrir un missatge de correu electrònic, es recomana comprovar que el remitent sigui algú conegut.

g) Per evitar el correu massiu no sol·licitat, com a regla general només s'ha de donar l'adreça de correu electrònic a persones conegudes.

h) No s'ha d'introduir l'adreça de correu electrònic en fòrums o llocs web no institucionals o que no siguin de confiança.

2. De forma no limitant, no s'accepten les activitats següents:

a) L'enviament de missatges de correu electrònic de correu brossa (per exemple, Ponzi o altres estafes piramidals) o altre material publicitari a persones que no hagin sol·licitat específicament aquest material.

b) L'enviament de missatges de correu electrònic que pel seu contingut incompleixi el marc normatiu del Principat d'Andorra.

Article 14. *Les publicacions en línia*

1. Les publicacions en línia que els usuaris facin en el marc de la seva tasca professional estan subjectes als termes i restriccions establerts en aquesta normativa.

2. Es permet l'ús limitat i ocasional dels sistemes de l'entitat per participar en publicacions en línia, sempre que es faci de manera professional i responsable, no infringeixi la normativa, no perjudiqui els interessos de l'entitat i no interfereixi en les tasques laborals habituals dels usuaris.

Article 15. *L'ús de l'emmagatzematge*

1. L'espai en disc i a la xarxa corporativa no s'ha d'emprar per a fins privats, ja que constitueix una eina de treball i té capacitat limitada. En particular, s'ha d'evitar emmagatzemar, fins i tot amb caràcter provisional o temporal, continguts de grans dimensions, com arxius multimèdia.

2. Com a mesura preventiva, en les estacions de treball i equips portàtils corporatius es restringeix l'entrada i la sortida de dades, i es limita l'accés als suports d'emmagatzematge.

3. Queda prohibit copiar informació en suports no gestionats.

4. L'emmagatzematge d'informació al núvol només s'efectua usant les plataformes aprovades i autoritzades.

Article 16. *L'ús d'impressores, fotocopiadores i escàners*

1. En cas d'enviar a imprimir un document amb informació confidencial a una impressora compartida amb més usuaris, l'usuari ha d'esperar que acabi la impressió presencialment per evitar pèrdues o oblits de la documentació.

2. Després de fotocopiar o escanejar un document, s'ha d'enretirar l'original i la còpia al moment.

3. Cal destruir les còpies en paper rebutjades que continguin informació confidencial en destructores de paper.

Dipòsit legal: AND.2-2015

Article 17. *La pèrdua de la vinculació laboral*
1. Els usuaris no poden esborrar informació dels dispositius digitals, de la xarxa, dels espais o dels serveis corporatius, d'aplicacions corporatives, de bústies de correu i de suports externs quan cessi la seva vinculació laboral o col·laboració professional amb el Consell Superior de la Justícia o l'Administració de justícia.

2. L'Àrea de Transformació Digital gestiona o elimina, d'acord amb els procediments establerts, els dispositius digitals i la informació i les aplicacions.

3. Es pot recuperar la informació dels serveis informàtics que es posen a disposició dels usuaris per a l'exercici de les seves funcions.

4. En finalitzar la relació laboral o la col·laboració professional, l'usuari ha de retornar immediatament tot el material de qualsevol tipus que li hagi estat lliurat.

Article 18. *Control en cas d'indicis d'ús indegut*
1. El Consell Superior de la Justícia pot fer les tasques de control i seguiment que siguin necessàries en les infraestructures comunes, dispositius digitals i serveis d'informació assignats als usuaris a l'efecte de comprovar i verificar que l'ús dels actius d'informació s'ajusta al que estableix aquest Reglament i no genera incidències operatives o de ciberseguretat.

2. Amb la finalitat de garantir el bon funcionament dels sistemes d'informació i de fer un seguiment de la seva utilització, així com de detectar els possibles incidents de seguretat i respondre-hi, es disposa d'eines i mitjans de control per fer el seguiment del seu ús i supervisar-lo, que permeten:

a) Registrar l'accés als dispositius digitals i aplicacions, als sistemes d'informació i a les infraestructures comunes.

b) Limitar l'accés a determinats webs o infraestructures comunes no relacionats amb les activitats laborals i registrar l'accés dels usuaris a Internet, les pàgines web visitades i l'hora de connexió.

c) Registrar el volum de correu electrònic enviat i rebut, quins són l'emissor i els destinataris dels missatges i bloquejar els missatges que puguin suposar una vulneració d'aquest Reglament o un risc de ciberseguretat.

d) Registrar l'ús de les comunicacions digitals dels usuaris, controlar el volum de tràfic de descàrrega de dades des d'Internet, i, si no és justificat, disminuir la velocitat de descàrrega sense avís previ.

e) Analitzar les aplicacions i els elements de la infraestructura comuna, els serveis i els dispositius digitals amb la finalitat de detectar i erradicar el codi maliciós i l'equipament informàtic que el creï, distribueixi o processi.

3. Es pot bloquejar i desconnectar qualsevol dispositiu digital o infraestructura comuna que suposi una amenaça per al bon funcionament dels sistemes d'informació o causi incidències.

Article 19. *Formació*
El Consell Superior de la Justícia ha de facilitar la formació necessària als usuaris interns als efectes del degut coneixement d'aquesta normativa.

Article 20. *Incompliment*
1. L'incompliment del que disposa aquest Reglament pot ser sancionat d'acord amb la Llei de la funció pública de l'Administració de justícia i la Llei qualificada de la justícia, sens perjudici que s'adoptin les mesures de restricció o de suspensió d'ús que es considerin escaients. En qualsevol cas, correspon als superiors jeràrquics prevenir i, si escau, corregir l'incompliment de les obligacions del personal en aquesta matèria.

2. En el cas d'incompliment del que determina aquest Reglament per part del personal extern, és aplicable el que estableixi el contracte de prestació de serveis, sens perjudici que es puguin adoptar les mesures de restricció o suspensió que es considerin adients, així com altres mesures orientades a efectuar les

Dipòsit legal: AND.2-2015

reclamacions a les quals aquest incompliment pugui donar lloc, en els termes establerts a la Llei de contractació pública o altra normativa aplicable.

Cosa que es fa pública per a coneixement general,

Andorra la Vella, 11 de desembre del 2024

Josep Maria Rossell Pons
President

Dipòsit legal: AND.2-2015