Agència Catalana de Notícies

Política de Seguretat

Editat	Revisat	Aprovat
Xavier Berga Congost	Responsable Seguretat	Comitè de Seguretat/Direcció
Data: 15/02/2024	Data: 22/02/2024	Data: 01/03/2024

Informació del document

Nom del procediment:	SI-NO-01 Política de Seguretat		
Descripció:			
Preparat per:	Xavier Berga Congost	**Versió del document:**	2.0
Rol:	Consultor de Seguretat	**Data de la versió del document:**	15/02/2024
		Data aprovació del document:	01/03/2024

Llista de distribució

DE	DATA	TELÈFON/@

PER A	ACCIÓ *	DATA ENTREGA	TELÈFON/@

** Tipus d'Acció: Aprovació, Revisió, Informat, Acció Requerida, Assistir a la reunió, Altres (si us plau, especificar)*

Historial de versions

No. Versió	Data versió	Revisat per	Descripció
1.0	21/02/2022	Xavier Berga Congost	Versió Inicial.
2.0	15/02/2024	Xavier Berga Congost	Adaptació de la Política de Seguretat al nou RD 311/2022.

Contingut

1. Exposició de Motius

Intracatalonia, S.A. (ACN) depèn dels Sistemes TIC (Tecnologies d'Informació i Comunicacions) per tal de aconseguir els seus objectius.
Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar a la disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat de la informació tractada o els serveis prestats.
L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.
Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat en prevenció del ús previst i valor de la informació i els serveis prestats.
Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per tal de garantir la continuïtat dels serveis prestats.
Els diferents departaments han d'assegurar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC. Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord a l'Article 7 de l'ENS.

Gestió d'incidents de seguretat

Prevenció

Els departaments han d'evitar, o almenys prevenir tant com sigui possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. L'ENS a través del seu article 19 estableix que els sistemes s'han de dissenyar i configurar de manera que garanteixin la seguretat per defecte, en línia amb la política de mínim privilegi “Need to Know”. De la mateixa manera, l'article 17 de l'ENS esmentat defineix que els sistemes s'instal·laran en àrees separades, dotades d'un procediment de control d'accés.
Per això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i les responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.
Per garantir el compliment de la política, els departaments han de:

- Establir àrees segures per als sistemes d’informació crítica o confidencial.
- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de forma rutinària.

- Sol·licitar la revisió periòdica per part de tercers per obtenir una avaluació independent.

Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, els serveis han de monitoritzar l'operació de manera contínua per detectar anomalies als nivells de prestació dels serveis i actuar en conseqüència segons això establert a l'article 8 de l'ENS.
La monitorització és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 de l'ENS. S'establiran mecanismes de detecció, anàlisi i reporti que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.
Els sistemes de detecció d'intrusos compleixen fonamentalment una tasca de supervisió i auditoria sobre els recursos de l'Organització, verificant que la política de seguretat no és violada i intenta identificar qualsevol tipus d'activitat maliciosa d'una manera primerenca i eficaç.
S'hauran d'establir, en funció de les necessitats, les classificacions següents:

- Sistemes de detecció d'intrusos a nivell de xarxa.
- Sistemes de detecció d'intrusos a nivell de sistema.

Resposta

Els departaments han de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions quant a incidents detectats en altres departaments o altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

Recuperació

Per garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i les activitats de recuperació corresponents.

Abast

Aquesta política aplica als Sistemes d'Informació següents associats a:

Esquema Nacional de Seguretat (Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat):

- Sistema d'informació propietat de Intracatalonia, S.A. (ACN) necessari per a la prestació adequada de serveis a la ciutadania relacionats amb: solucions de seu electrònica com la carpeta ciutadana, registre telemàtic, tràmits electrònics, portals de proveïdors, portal de l'empleat, perfil del contractant i notificacions. Sistema de gestió de contractació, gestor documental, arxiu i

notificacions electròniques, gestió patrimonial, nòmines i gestió de recursos humans, cadastre i GIS, padró, registres, subvencions i solucions mòbils.

Missió i Serveis Prestats

Intracatalonia, S.A. (ACN) com a Òrgan de Govern Municipal, per a la gestió dels seus interessos, i en l'àmbit de les seves competències i com a Administració pública, serveix amb objectivitat els interessos generals i actua d'acord als principis d'eficàcia, jerarquia, descentralització i coordinació, promou tota classe d'activitats i presta els serveis públics que contribueixen a satisfer les necessitats i aspiracions dels habitants del municipi.

Marc Normatiu

Com a base normativa per realitzar aquesta política de seguretat, s'ha analitzat la legislació vigent, que afecta el desenvolupament de les activitats de l'Administració Local, en el què es refereix a Administració electrònica, i que implica la implantació de forma explícita de mesures de seguretat als sistemes d'informació. El marc legal en matèria de seguretat de la informació ve establert per la següent legislació:

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic.
- Reial decret 209/2003, de 21 de febrer, pel qual es regulen els registres i les notificacions telemàtiques, així com la utilització de mitjans telemàtics per a la substitució de l'aportació de certificats pels ciutadans.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

Veure document: ***Marc normatiu de seguretat.***

Procediment Administratiu

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

Protecció de Dades de Caràcter Personal

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en què respecta al tractament de dades personals a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- DIRECTIVA (UE) 2016/680 DEL PARLAMENT EUROPEU I DEL CONSELL de 27 d'abril del 2016 relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la qual es deroga la Decisió Marc 2008/977/JAI del Consell.
- Llei 3/2018, del 5 de desembre, de Protecció de Dades de Caràcter Personal i Garantia dels Drets Digitals.

Administració Electrònica

- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat a l'àmbit de l'Administració Electrònica.
- Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell (Identificació electrònica i serveis de confiança per a les transaccions electròniques al mercat interior)
- La Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

Signatura Electrònica

- Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior i pel qual es deroga la Directiva 1999/93 /CE.
- COM (2001) 298 - final, de la Comissió Europea - Seguretat de les xarxes i de la informació: Proposta per a un enfocament polític europeu.
- Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

Seguretat de les Xarxes i de la Informació

- Guies de l'OCDE per a la seguretat dels sistemes d'informació i de xarxes. Cap a una cultura de seguretat. Com a complement a la legislació vigent, actualment existeix la norma internacional UNE ISO/IEC 27002 “Codi de Bones Pràctiques per a la gestió de la seguretat de la informació” que s'ha configurat com un estàndard a l'hora d'auditar els aspectes relacionats amb la seguretat de la informació a les organitzacions.

Organització de la Seguretat

Comitès: Funcions i Responsabilitats

El Comitè de Seguretat és l’Òrgan que coordina la Seguretat de la Informació a nivell d’Organització.

Estarà constituït pel Responsable de Seguretat de la Informació i representants d' altres àrees afectades per l'ENS.

Funcions Associades

- Responsabilitats derivades del tractament de dades de caràcter personal.
- Assumpció de la figura de Responsable de Servei per a tots els serveis prestats en el marc de la RD 311/2022.
- Assumpció de la figura de Responsable de la Informació per a totes les informacions emprades pels serveis prestats en el marc de la RD 311/2022.
- Atendre les inquietuds dels Òrgans superiors competents i dels diferents departaments.
- Informar regularment de l'estat de la seguretat de la informació els òrgans superiors competents.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació.

- Elaborar l'estratègia devolució de l'Organització quant a la seguretat de la informació.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada pels Òrgans superiors competents.
- Aprovar la normativa de seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Monitoritzar els riscos residuals principals assumits per l'Organització i recomanar possibles actuacions al respecte.
- Monitoritzar l'exercici dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions al respecte. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
- Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Aprovar plans de millora de la seguretat de la informació de l'organització. En particular, vetllarà per la coordinació de diferents plans que es puguin fer en diferents àrees.
- Vetllar perquè la seguretat de la informació es té en compte en tots els projectes TIC des de la seva especificació inicial fins a la posada en operació. En particular, haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents àrees de l'Organització, elevant aquells casos en què no tingui prou autoritat per decidir.

En cas d'Ocurrència d'Incidents de Seguretat de la Informació

Aprovarà el Pla de millora de la seguretat, amb la dotació pressupostària corresponent. El Comitè de Seguretat de la Informació no és un comitè tècnic, però demanarà regularment del personal tècnic, propi o extern, la informació pertinent per prendre decisions.
El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals hagi de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, podent materialitzar-se de diferents formes i maneres:

- Grups de treball especialitzats interns, externs o mixtos.
- Assessoria externa.
- Assistència a cursos o altres tipus d'entorns formatius o d'intercanvi d'experiències.

El Responsable de la Seguretat de la Informació és el secretari del Comitè de Seguretat de la Informació i com a tal:

- Convoca les reunions del Comitè de Seguretat de la Informació.
- Prepara els temes a tractar a les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elabora l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.

Definició de rols

La Política de Seguretat, segons requereix l'Annex II de l'Esquema Nacional de Seguretat a la secció 3.1, ha d'identificar uns clars responsables per vetllar pel seu compliment i ser coneguda per tots els membres de l'organització Administrativa.

S'estableixen els rols següents a l'organització relacionats amb la Seguretat de la Informació.

Responsable de la Informació

Correspon al nivell d'un Òrgan de Govern de màxim nivell, constituït pels Òrgans superiors competents, que entén la missió de l'organització, determina els objectius que es proposa assolir i respon que s'aconsegueixin.
Les seves funcions poden ser assignades a persones individuals, o bé ser assumides pel Comitè de Seguretat de la Informació.
La persona o òrgan que ho assumeixi haurà de ser identificada per a cada informació que tracti l'organització.

Funcions Associades

- Té la responsabilitat última de l'ús que es faci duna certa informació i, per tant, de la seva protecció.
- El Responsable de la Informació delega al Comitè de Seguretat com a responsable de qualsevol error o negligència que porti a un incident de confidencialitat o d'integritat.
- Estableix els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.
- El Responsable de la Informació delega al Responsable de cadascun dels Actius com a responsable de Determinar els nivells de seguretat en cada dimensió dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.
- Tot i que l'aprovació formal dels nivells correspongui al Responsable de la Informació, podrà demanar una proposta del Responsable de la Seguretat i del Responsable del Sistema.

Compatibilitat amb altres Rols

Aquest rol podrà coincidir amb el del Responsable de Servei i amb el de Responsable del tractament requerit pel RGPD.
Aquest rol no podrà coincidir amb el de Responsable de Seguretat, excepte en organitzacions de dimensió reduïda que funcionin de forma autònoma.
Aquest rol no pot coincidir amb el de Responsable de Sistema ni amb el d'Administrador de la Seguretat del Sistema, ni tan sols quan es tracti d'organitzacions de dimensió reduïda que funcionin de manera autònoma.

Responsable del Servei

Quan sigui diferent del Responsable de la Informació, pot correspondre al nivell d'un Òrgan de Govern de màxim nivell, igual que el Responsable de la Informació, o bé al d'una Direcció executiva o gerència, que entén què fa cada departament, i com els departaments es coordinen entre si per assolir els objectius marcats pels Òrgans superiors competents.
Les seves funcions poden ser assignades a persones individuals, o bé ser assumides pel Comitè de Seguretat de la Informació.
El Responsable del Servei delega al Responsable de cadascun dels Actius com a responsable de Determinar els nivells de seguretat en cada dimensió dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.
La persona o òrgan que ho assumeixi haurà de ser identificada per a cada servei que presti l'organització.

Funcions Associades

- Estableix els requisits dels serveis en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.
- Té la responsabilitat última de l'ús que es faci de determinats serveis i, per tant, de la seva protecció.
- El Responsable del servei és el responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis.
- Determinarà els nivells de seguretat en cada dimensió del servei dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.
- Encara que l'aprovació formal dels nivells correspongui al Responsable del Servei, podrà demanar una proposta del Responsable de la Seguretat i del Responsable del Sistema.
- La prestació d'un servei sempre ha d'atendre els requisits de seguretat de la informació que maneja, de manera que en poden heretar els requisits de seguretat, afegint-hi requisits de disponibilitat, així com altres com accessibilitat, interoperabilitat, etc.

Compatibilitat amb altres Rols

Podrà coincidir en la mateixa persona o òrgan el rol de Responsable de la Informació i del Responsable del Servei, encara que generalment no coincidiran quan:

- El servei gestioni informació de diferents procedències, no necessàriament de la mateixa unitat departamental que la que presta el servei.
- La prestació del servei no depengui de la unitat a què pertany el Responsable de la Informació.
- Aquest rol podrà coincidir amb el del Responsable de Servei i amb el de Responsable de Fitxer requerit pel RGPD.
- Aquest rol no podrà coincidir amb el de Responsable de Seguretat, excepte en organitzacions de dimensió reduïda que funcionin de forma autònoma.
- Aquest rol no pot coincidir amb el de Responsable de Sistema ni amb el d'Administrador de la Seguretat del Sistema, ni tan sols quan es tracti d'organitzacions de dimensió reduïda que funcionin de manera autònoma.

Responsable de Seguretat de la Informació

Correspon al nivell d'una direcció executiva.

Es nomenarà formalment com a tal una única persona a l'organització. El rol no podrà ser desenvolupat per un òrgan col·legiat, ni hi podrà haver més duna persona assumint el rol en l'organització, encara que pugui delegar part de les seves funcions en altres persones.

F uncions Associades

- Reportarà directament el Comitè de Seguretat de la Informació.
- Actuarà com a secretari del Comitè de Seguretat de la Informació.
- Convocarà el Comitè de Seguretat de la Informació, recopilant la informació pertinent.
- Pertanyerà al Comitè de Seguretat Corporativa, per coordinar les necessitats de Seguretat de la Informació en el marc de la resta de necessitats de Seguretat Corporativa.
- Mantindrà la seguretat de la informació emprada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, segons el que estableix la Política de Seguretat de l'Organització.

- Promourà la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
- Recopilarà els requisits de seguretat dels Responsables d'Informació i del Servei i determinarà la categoria del Sistema.
- Realitzarà l'Anàlisi de Riscos.
- Elaborarà una Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides d'acord amb l'Annex II de l'ENS i el resultat de l'Anàlisi de Riscos.
- Facilitarà als Responsables d'Informació i als Responsables de Servei informació sobre el nivell de risc residual esperat després d'implementar les opcions de tractament seleccionades en l'anàlisi de riscos i les mesures de seguretat requerides per l'ENS.
- Coordinarà l'elaboració de la documentació de seguretat del sistema.
- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per aprovar-la la Direcció.
- Participarà en l'elaboració i l'aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.
- Elaborarà i aprovarà els procediments operatius de seguretat de la informació.
- Facilita periòdicament al Comitè de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i de l'estat de la seguretat del sistema (en particular del nivell de risc residual a què està exposat el sistema).
- Elaborarà, juntament amb els Responsables de Sistemes, Plans de Millora de la Seguretat, per a la seua aprovació pel Comitè de Seguretat de la Informació.
- Elaborarà els plans de formació i conscienciació del personal en Seguretat de la Informació, que hauran de ser aprovats pel Comitè de Seguretat de la Informació.
- Validarà els Plans de Continuïtat de Sistemes que elabori el Responsable de Sistemes, que hauran de ser aprovats pel Comitè de Seguretat de la Informació i provats periòdicament pel Responsable de Sistemes.
- Aprovarà les directrius proposades pels Responsables de Sistemes per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.

En cas d'ocurrència d'incidents de seguretat de la informació

- Analitzarà i proposarà Salvaguardes que previnguin incidents semblants en un futur.

Compatibilitat amb altres Rols

Aquest rol només pot coincidir amb la del Responsable de Servei i el Responsable d'Informació en organitzacions de dimensions reduïdes que tinguin una estructura autònoma de funcionament.

Aquest rol no pot coincidir amb el de Responsable de Sistema i amb l'Administrador de Seguretat del Sistema, encara que es tracti d'organitzacions de dimensions reduïdes que tinguin una estructura autònoma de funcionament.

Delegació de Funcions

Per determinats Sistemes d'Informació que, per la seva complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessiti personal addicional per dur a terme les funcions de Responsable de la Seguretat, es podran designar els Responsables de Seguretat Delegats que es considerin necessaris.

La designació correspon al Responsable de la Seguretat. Per mitjà de la designació de delegats, es deleguen funcions. La responsabilitat final continuarà recaient sobre el Responsable de la Seguretat.
Els Responsables de Seguretat Delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegui el Responsable de la Seguretat, i pot ser, per exemple, la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals.
Cada Responsable de Seguretat Delegat tindrà una dependència funcional directa del Responsable de la Seguretat, que és qui reporten.
La delegació de funcions passarà prèviament pel comitè.

Responsable del Sistema

Correspon al nivell d'una direcció operativa.
Es nomenarà formalment com a tal una única persona per a cada sistema. El rol no podrà ser desenvolupat per un òrgan col·legiat, encara que pugui delegar part de les funcions en altres persones.

Funcions Associades

Les seves funcions seran les següents:

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el cicle de vida, de les especificacions, instal·lació i verificació del funcionament correcte.
- Definir la topologia i el sistema de gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.
- Assegureu-vos que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- El Responsable del Sistema pot acordar la suspensió de l'ús duna certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsables de la informació afectada, del servei afectat i amb el responsable de la seguretat abans de ser executada.
- Aplicar els procediments operatius de seguretat elaborats i aprovats pel responsable de seguretat.
- Monitoritzar l'estat de la seguretat del Sistema d'Informació i reportar-lo periòdicament o davant d'incidents de seguretat rellevants al Responsable de Seguretat de la Informació.
- Elaborar els Plans de Continuïtat del Sistema perquè siguin validats pel Responsable de Seguretat de la Informació, i coordinats i aprovats pel Comitè de Seguretat de la Informació.
- Realitzar exercicis i proves periòdiques dels Plans de Continuïtat del Sistema per mantenir-los actualitzats i verificar que són efectius.
- Elaborarà les directrius per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos (especificació, arquitectura, desenvolupament, operació i canvis) i les facilitarà al Responsable de Seguretat de la Informació per aprovar-la.

En cas d'Ocurrència d'Incidents de Seguretat de la Informació

- Planificarà la implantació de les Salvaguardes al sistema.
- Executarà el pla de seguretat aprovat.

Compatibilitat amb altres Rols

Aquest rol no podrà coincidir amb el de Responsable d'Informació, ni amb el de Responsable de Servei.
Aquest rol pot coincidir amb el d'administrador de seguretat del sistema en organitzacions d'una dimensió reduïda o mitjana que tinguin una estructura autònoma de funcionament.
En grans organitzacions no hauria de coincidir amb el d'administrador de la seguretat del sistema, independentment de la mida del sistema.

Administrador de la Seguretat del Sistema

Correspon al nivell d'un empleat qualificat de seguretat informàtica de sistemes.
Podrà nomenar-se formalment com a tals diverses persones per a cada sistema. El rol no podrà ser desenvolupat per un òrgan col·legiat, ni podrà delegar part de les funcions en altres persones.
Si escau, es nomenarien nous Administradors de la Seguretat del Sistema.
Serà proposat pel Responsable del Sistema, a qui reportarà en tot allò relacionat amb seguretat de la informació.

Funcions Associades

- La implementació, la gestió i el manteniment de les mesures de seguretat aplicables al Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són estrictament complerts.
- Assegurar que la traçabilitat, les pistes d'auditoria i altres registres de seguretat requerits estiguin habilitats i registrin amb la freqüència desitjada, d'acord amb la política de seguretat establerta per l'Organització.
- Aplicar als sistemes, usuaris i altres actius i recursos relacionats amb aquest, tant interns com externs, els procediments operatius de seguretat i els mecanismes i serveis de seguretat requerits.
- Assegurar que són aplicats els procediments aprovats per manejar el sistema d'informació i els mecanismes i serveis de seguretat requerits.
- La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat del Sistema d'Informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.
- Aprovar els canvis a la configuració vigent del Sistema d'Informació, garantint que segueixin operatius els mecanismes i serveis de seguretat habilitats.
- Informar els Responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Monitoritzar l'estat de seguretat del sistema.

En cas d'Ocurrència d'Incidents de Seguretat de la Informació

- Dur a terme el registre, la comptabilitat i la gestió dels incidents de seguretat en els sistemes sota la seva responsabilitat.
- Executar el pla de seguretat aprovat.
- Aïllar l'incident per evitar la propagació a elements aliens a la situació de risc.
- Prendre decisions a curt termini si la informació s'ha vist compromesa de manera que pogués tenir conseqüències greus (aquestes actuacions haurien d'estar documentades per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).

- Assegurar la integritat dels elements crítics del Sistema si s'ha vist afectada la disponibilitat en aquests (aquestes actuacions quedaran documentades per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Mantenir i recuperar la informació emmagatzemada pel sistema i els seus serveis associats.
- Investigar l'incident: Determineu la manera, els mitjans, els motius i l'origen de l'incident.

Compatibilitat amb altres Rols

Aquest rol no podrà coincidir amb el de Responsable d'Informació, amb el de Responsable de Servei ni amb el de Responsable de Seguretat Corporativa o de la Informació.
Aquest rol podrà coincidir amb el de Responsable del Sistema en organitzacions de dimensió reduïda o mitjana que tinguin una estructura autònoma de funcionament.
En grans organitzacions no hauria de coincidir amb el de Responsable del Sistema, independentment de la mida del Sistema.

Delegació de Funcions

En determinats sistemes d'informació que per la seva complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessiti de personal addicional per dur a terme les seves funcions, es podran designar Administradors de Seguretat del Sistema Delegats.
Els administradors de seguretat del sistema Delegats seran responsables, en el seu àmbit, d'aquelles accions que delegui l'administrador de seguretat del sistema relacionades amb la implantació, la gestió i el manteniment de les mesures de seguretat aplicables al sistema d'informació.
L'administrador de seguretat del sistema delegat serà designat a sol·licitud de l'administrador de seguretat del sistema, del qual dependrà funcionalment.
La delegació de funcions passarà prèviament pel comitè.
La vostra identitat apareixerà reflectida a la documentació de seguretat del sistema d'informació.

Responsable en matèria de protecció de dades

Designació d'un Delegat de Protecció de Dades:

L'article 37 del RGPD estableix que el responsable i l'encarregat del tractament han de designar un delegat de protecció de dades sempre que:

a) El tractament el porti a terme una autoritat o organisme públic, excepte els tribunals que actuïn en exercici de la seva funció judicial;

b) Les activitats principals del responsable o de l'encarregat consisteixin en operacions de tractament que, per raó de la seva naturalesa, abast i/o fins, requereixin una observació habitual i sistemàtica d'interessats a gran escala, o

c) Les activitats principals del responsable o de l'encarregat consisteixin en el tractament a gran escala de categories especials de dades personals d'acord amb l'article 9 i de dades relatives a condemnes i infraccions penals a què fa referència l'article 10.

Article 39 del RGPD:

El delegat de protecció de dades tindrà com a mínim les funcions següents:

a) Informar i assessorar el responsable o l'encarregat del tractament i els empleats que s'ocupin del tractament, de les obligacions que els incumbeixen en virtut d'aquest Reglament i altres disposicions de protecció de dades de la Unió o dels estats membres.

b) Supervisar el compliment del que disposa aquest Reglament, altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i la formació del personal que participa en les operacions de tractament, i les auditories corresponents.

c) Oferir l'assessorament que se us demani sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació de conformitat amb l'article 35 del reglament.

d) Cooperar amb l'autoritat de control.

e) Actuar com a punt de contacte de la corresponent Autoritat de Control per a qüestions relatives al tractament, inclosa la consulta prèvia a què fa referència l'article 36 del reglament, i fer consultes, si escau, sobre qualsevol altre assumpte.

Segons el RGPD, la posició del DPO/DPD comporta:

- La participació de manera adequada i en temps oportú en totes les qüestions relatives a la protecció de dades personals.
- Rebre el suport del responsable o encarregat, que li han de facilitar els recursos necessaris per al compliment de les seves funcions.
- No rebre cap instrucció quant a l'exercici d'aquestes funcions i no ser destituït ni sancionat pel responsable o l'encarregat per causes relacionades amb aquest exercici de funcions.
- Retre comptes directament al més alt nivell jeràrquic del responsable o encarregat.
- Aquesta característica s'ha d'interpretar en el sentit que el DPD s'ha de poder relacionar amb nivells jeràrquics que tinguin la capacitat d'adoptar o promoure decisions basades en les recomanacions, les propostes o les avaluacions que faci el DPD.

Dades de Caràcter Personal

Intracatalonia, S.A. (ACN) tracta dades de caràcter personal.

Veure: ***Registre d'Activitats del Tractament (RAT)*** on es recullen els Fitxers afectats i els corresponents Responsables.
Tots els sistemes d'informació de Intracatalonia, S.A. (ACN) s'ajustaran als nivells de seguretat requerits per el Reglament, a fi i efecte, de la naturalesa i la finalitat de les dades de caràcter personal recollides.

Gestió de Riscos

Justificació

Tots els sistemes subjectes a aquesta Política hauran de fer una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats.
L'anàlisi de riscos serà la base per determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establerts per l'Esquema Nacional de Seguretat, segons el que preveu l'article 7 de l'ENS.

Criteris d'avaluació de riscos

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació manejada i els diferents serveis prestats.
Els criteris d'avaluació de riscos detallats s'especificaran a la metodologia d'avaluació de riscos que elaborarà l'organització, basant-se en estàndards i bones pràctiques reconegudes.
S'han de tractar, com a mínim, tots els riscos que puguin impedir la prestació dels serveis o el compliment de la missió de l'organització de manera greu.
Es prioritzaran especialment els riscos que impliquin un cessament en la prestació dels serveis prestats.

Directrius de tractament

El Comitè de Seguretat de la Informació dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

Procés d'acceptació del Risc Residual

Els Riscos Residuals seran determinats pel Responsable de Seguretat de la Informació.
Els nivells de risc residuals esperats sobre cada informació després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes a l'annex II de l'ENS) hauran de ser acceptats prèviament pel seu responsable d'aquesta informació.
Els nivells de Risc residuals esperats sobre cada Servei després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes a l'Annex II de l'ENS) i hauran de ser acceptats prèviament pel Responsable de aquest Servei.
Els nivells de Risc Residuals seran presentats pel Responsable de Seguretat de la Informació al Comitè de Seguretat de la Informació, perquè aquest sigui procedent, si escau, a avaluar, aprovar o rectificar les opcions de tractament proposades.

Necessitat de fer o actualitzar avaluacions de riscos

L'anàlisi dels riscos i el seu tractament ha de ser una activitat repetida regularment, d'acord amb el que estableix l'article 7 de l'ENS. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan es produeixin canvis significatius a la informació manejada.
- Quan es produeixin canvis significatius als serveis prestats.
- Quan es produeixin canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.
- Quan es produeixi un incident greu de seguretat.

- Quan es reportin vulnerabilitats greus.

Obligacions del Personal

Tots els membres de l'Organització tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat; és responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi als afectats.
El compliment de la present Política de Seguretat és obligatori per part de tot el personal intern o extern que intervingui en els processos de l'organització, constituint-ne l'incompliment, la infracció greu a efectes laborals, d'acord amb el conveni col·lectiu laboral.

Vegeu la Normativa de Seguretat Interna: ***FOP - Funcions i Obligacions del Personal***

Formació i Conscienciació del Personal

L'objectiu de Intracatalonia, S.A. (ACN) és conscienciar de forma contínua la Ciberseguretat dels empleats, per això, es realitzen les següents activitats:

- Formació inicial a la incorporació dels empleats a l'organització
- Enviament trimestral de píndoles de conscienciació a Ciberseguretat.
- Enviament puntual de píndoles informatives de Ciberseguretat, responent a situacions de risc.
- Formació anual a tot el personal d'actualització en Ciberseguretat.
- Formació específica segons el lloc de treball i necessitats concretes.

La Direcció es compromet a la Formació i Conscienciació de tot el personal de Intracatalonia, S.A. (ACN).

Terceres parts

Quan es prestin serveis o es gestioni informació altres organitzacions, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals de reporti i coordinació dels Comitès de Seguretat de la Informació respectius i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.
Quan s'utilitzin serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat (FOP) que concerneixi aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i podrà desenvolupar els seus propis procediments operatius per satisfer-la.
S'establiran procediments específics de reporti i resolució d'incidències.
Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que estableix aquesta Política.
Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es requereix als paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que necessiti els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

Revisió i Aprovació de la Política de Seguretat

La Política de Seguretat de la Informació serà revisada pel Comitè de Seguretat de la Informació a intervals planificats, que no podran excedir l'any de durada, o sempre que es

produeixin canvis significatius, per tal d'assegurar que se'n mantingui la idoneïtat, l'adequació i eficàcia.
Els canvis sobre la Política de Seguretat de la Informació hauran de ser aprovats per l'òrgan superior competent que correspongui, d'acord amb l'article 11, al Capítol III Article 12 de l'ENS.

Qualsevol canvi sobre aquesta haurà de ser difós a totes les parts afectades.

La Política de Seguretat estarà Notificada, Comunicada i disponible per a tot el personal de Intracatalonia, S.A. (ACN).

Anna Nogué Regàs - DNI 40311538J (TCAT)

Firmado digitalmente por Anna Nogué Regàs - DNI 40311538J (TCAT)
Nombre de reconocimiento (DN): c=ES, o=Intracatalònia, S.A., 2.5.4.97=VATES-A61844411, ou=Treballador públic de nivell alt, sn=Nogué Regàs - DNI 40311538J, givenName=Anna, serialNumber=IDCES-40311538J, cn=Anna Nogué Regàs - DNI 40311538J (TCAT)
Fecha: 2024.03.01 13:23:13 +01'00'