Revisió: 0
Data publicació: 18.11.2022

POLÍTICA DE SEGURETAT ESQUEMA NACIONAL DE SEGURETAT (ENS)

1. APROBACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 1 de setembre de 2021 per la Direcció.

Aquesta Política de Seguretat de la Informació és efectiva des d'aquesta data i fins que siga reemplaçada per una nova Política.

2.INTRODUCCIÓ

CIUTAT DE LES ARTS I LES CIÈNCIES, d'ara en avant CAC, depén entre altres, dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per a aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguen afectar la disponibilitat, integritat o confidencialitat 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 de manera ràpida i eficient enfront dels incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per a defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn per a 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 a garantir la continuïtat dels serveis prestats.

Les diferents Direccions i Àrees han de cerciorar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seua concepció fins a la seua 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 i en la sol·licitud d'ofertes.

CAC ha d'estar preparada per a previndre, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'Article 7 del ENS.

2.1 PREVENCIÓ

CAC ha d'evitar, o almenys previndre en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a això s'ha d'implementar les mesures mínimes de seguretat determinades pel ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i

responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats. Per a garantir el compliment de la política, els departaments de l'Àrea de Sistemes deuen:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de manera rutinària.
- Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtindre una avaluació independent.

2.2. DETECCIÓ

Atés que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple degradació fins a la seua detenció, els serveis han de monitorar l'operació de manera contínua per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que s'estableix en l'Article 9 del ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'Article 8 del ENS. S'establiran mecanismes de detecció, anàlisi i reporte que arriben als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagen preestablit com a normals.

2.3. RESPOSTA

Els diferents departaments de l'Àrea de Sistemes deuen:

- Establir mecanismes per a respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en 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).

2.4. RECUPERACIÓ

Per a garantir la disponibilitat dels serveis crítics, l'Àrea de Sistemes ha de desenvolupar plans de continuïtat dels sistemes TIC com a part del pla general de continuïtat de negoci i activitats de recuperació.

3. ABAST

Aquesta política s'aplica a tots els sistemes TIC de i a tot el personal de CAC, sense excepcions.

4. MISSIÓ I VISIÓ

Missió: Oferir a la societat uns continguts culturals i d'entreteniment, innovadors i de qualitat per al seu enriquiment intel·lectual i gaudi, en un conjunt arquitectònic avantguardista únic en

el món. Tot això, buscant sempre satisfer les necessitats i expectatives de tots els seus grups d'interés en general, i en particular dels valencians.

Visió: A la Ciutat de les Arts i las Ciències perseguim ser un referent a nivell internacional de:

- Divulgació cultural,
- Sostenibilitat i
- Turisme de Qualitat

I ser l'espai públic de trobada i oci dels valencians, tot això, mitjançant una gestió excel·lent que s'anticipe i adapte al canvi, basada en l'aprenentatge i la innovació permanent.

Valors:

- ÈTICA en totes les nostres actuacions. Integritat. Transparència. Igualtat. Respecte mutu.
- CONSCIÈNCIA DE SERVEI CAP A la SOCIETAT. El nord que guia les nostres actuacions és la creació de valor amb repercussió en la societat, en particular la valenciana, i en les empreses i institucions vinculades o afectades per la nostra activitat, donat el nostre caràcter d'empresa pública.
- RIGOR CIENTÍFIC. Precisió en el desenvolupament i divulgació dels continguts de la Ciutat de les Arts i les Ciències.
- ORIENTACIÓ Als NOSTRES VISITANTS. Aconseguir la plena satisfacció dels nostres visitants, tant a nivell empresarial i institucional com a nivell individual.
- COMPROMÍS SOCIAL I MEDIAMBIENTAL. Contribuïm al desenvolupament sostenible en totes les actuacions de la Ciutat de les Arts i les Ciències.
- INTERÉS PER LES PERSONES QUE INTEGREN L'EQUIP. Promovem un clima de treball en equip, integrat per persones compromeses, i ens preocupem per la igualtat, reconeixement, creixement i desenvolupament professional.
- INNOVACIÓ I MILLORA CONTÍNUA. El personal de la Ciutat de les Arts i les Ciències ha de ser emprenedor, adoptant una actitud activa, dinàmica i innovadora per a la millora contínua i la creació de valor afegit. Se li demana implicació, treball en equip i respecte als valors de l'organització.

5. MARC NORMATIU

CIUTAT DE LES ARTS I LES CIÈNCIES es troba subjecte a la següent normativa en la provisió dels serveis prestats als seus clients:

- Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.
- REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (reglament General de Protecció de Dades), d'aplicació al tractament totalment o parcialment automatitzat de dades personals, així com al tractament no automatitzat de dades personals continguts o destinats a ser inclosos en un fitxer.
- Prevenció de Riscos Laborals Llei 31/1995 de 8 de novembre i Reial decret 39/1997 de 17 de gener, pel qual s'aprova el Reglament dels Serveis de Prevenció.
- El conveni col·lectiu aplicable, corresponent a “Oficines i Despatxos”.

- Llei 34/2002, d'11 de juliol, de Serveis de la Societat de la Informació i Comerç Electrònic (LSSI-CE).
- RD-llei 13/2012 de 30 de març, llei de cookies.
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de Propietat Intel·lectual, regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria.

El marc de referència que dona cobertura legal a aquest document s'estableix en les següents seccions del Reial decret 3/2010 de 8 de gener, modificat pel RD 951/2015, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (d'ara en avant, ENS):

- ENS. Article 12. Organització i implantació del procés de seguretat

La seguretat haurà de comprometre a tots els membres de l'organització. La política de seguretat segons es detalla en l'Annex II, secció 3.1, haurà d'identificar uns clars responsables de vetlar pel seu compliment i ser coneguda per tots els membres de l'empresa.

- ENS. Annex II. Mesures de Seguretat Marc organitzatiu [org] Política de seguretat [org.1]

6. ORGANITZACIÓ DE LA SEGURETAT

6.1. COMITÉ: FUNCIONS I RESPONSABILITATS

El Comité de Gestió de la Seguretat de la Informació estarà format per la Coordinadora del Sistema Integrat de Gestió, el Director de Seguretat de la Informació, el Responsable Tècnic de Seguretat de la Informació, i el personal de l'Àrea de Sistemes.

El Comité té les funcions següents:

- Revisar periòdicament la política de seguretat tenint en compte els canvis en l'entorn i en la infraestructura TIC de CAC i proposar al Responsable del Sistema de Gestió les modificacions pertinents en la mateixa.
- Mantindre actualitzades les normatives de compliment obligatori en CAC.
- Establir plans de formació i informació que garantisquen que el personal de CAC coneix els riscos en esta matèria i sap com minimitzar-los.
- Organitzar, de forma periòdica les auditories tècniques de seguretat per a verificar el compliment de les normatives. Definir el pla de vigilància de les mateixes actuant inclús amb tècniques d'enginyeria social per a comprovar el seu compliment.
- Vetlar per l'eficàcia i eficiència dels controls i salvaguardes implantades.
- Marcar les hipòtesis de partida i l'abast per al desenrotllament d'auditories tècniques de seguretat internes o externes en matèria de seguretat (incloses les auditories biennals del Reglament de Mesures de Seguretat de la LOPD)
- Analitzar les incidències de seguretat i escalar, si es considera oportú, al Responsable del Sistema de Gestió o al responsable d'àrea corresponent, els incidents que requerisquen actuacions d'índole intern ja siga en aspectes disciplinaris o de comunicació interna o externa.
- Revisar l'anàlisi de riscos i comunicar els riscos residuals per a la seua aprovació i trasllat al Responsable del Sistema de Gestió.
- Proposar al Responsable del Sistema de Gestió projectes i iniciatives dissenyats per a minimitzar el nivell de risc identificat.

6.2. ROLS: FUNCIONS I RESPONSABILITATS

Els diferents rols junt amb les seues respectives funcions i responsabilitats estan reflectits en els procediments del sistema de gestió de documentació de qualitat “Qdoc”, documents:

- MO-SI-01 MANUAL DE FUNCIONS I RESPONSABILITATS DE SEGURETAT DE LA INFORMACIÓ
- MO-SGP-01 MANUAL DE ROLS I RESPONSABILITATS RGPD

6.3. PROCEDIMENTS DE DESIGNACIÓ

El Director de Seguretat de la Informació serà anomenat per la Direcció General de l'empresa, a proposta del Comité de Gestió de la Seguretat de la Informació. El nomenament es revisarà cada 4 anys o quan el lloc quede vacant.

6.4. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Serà missió del Comité de Gestió de Seguretat de la Informació la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. La Política serà aprovada pel mateix comité i difosa perquè la coneguen totes les parts afectades.

7. DADES DE CARÀCTER PERSONAL

CIUTAT DE LES ARTS I LES CIÈNCIES tracta dades de caràcter personal. El document de seguretat, a què tindran accés només les persones autoritzades, arreplega els fitxers afectats i els responsables corresponents. Tots els sistemes d'informació de CIUTAT DE LES ARTS I LES CIÈNCIES s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal arreplegats en el mencionat Document de Seguretat.

8. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política formaran part d'una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats. Esta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan canvie la informació manejada.
- Quan canvien els servicis prestats.
- Quan ocórrega un incident greu de seguretat.
- Quan es reporten vulnerabilitats greus.

Per a la valoració de l'anàlisi de riscos, el Comité de Gestió de la Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents servicis prestats. El Comité de Gestió de la Seguretat de la Informació dinamitzarà la disponibilitat de recursos per a atendre a les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

9. GESTIÓ DOCUMENTAL

Les directrius per a l'estructuració de la documentació del sistema, la seua gestió i accés es troben documentades en el procediment PC-PLC-01 CONTROL DE LA DOCUMENTACIÓ."

10. DESENROTLLAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta Política de Seguretat de la Informació complementa les polítiques de seguretat de CIUTAT DE LES ARTS I LES CIÈNCIES en diferents matèries:

- PSI-SI-01 AUDITORIA TECNOLÒGICA DE SEGURETAT DE LA INFORMACIÓ. Definix el procediment a aplicar per a l'execució i tractament dels resultats d'auditories internes de seguretat tecnològica, tant planificades com extraordinàries, dins de CAC, de manera que es garantisca permanentment la integritat, disponibilitat i confidencialitat dels recursos corporatius i la millora contínua dels sistemes de gestió implantats.
- PSI-SI-02 CONTROL DE SISTEMES EN OPERACIÓ. Descriu els mecanismes de control dels sistemes d'informació en CAC, per a garantir els nivells de qualitat i seguretat en la seua operació diària adequats a les necessitats de l'organització.
- PSI-SI-03 CALIBRATGE. Definix els mecanismes de calibratge del sistema de gestió d'esdeveniments de CAC, emas, per a garantir el seu funcionament correcte en l'entorn de treball de l'organització.
- PSI-SI-04 CONTROL DE CANVIS. Determina les tasques a realitzar per a garantir el control adequat dels canvis operacionals sobre els actius relacionats amb la seguretat dels sistemes d'informació de CAC; ja que un control incorrecte dels esmentats canvis és causa habitual de fallades de seguretat o del sistema.
- PSI-SI-05 GESTIÓ DE SUPORTS DE CÒPIES DE SEGURETAT. Definix els mecanismes de gestió de suports que contenen dades resultants de realitzar les còpies de seguretat dels servidors gestionats per l'Àrea de Sistemes.
- PSI-SI-06 GESTIÓ D'INCIDENTS DE SISTEMES D'INFORMACIÓ. Definix la gestió d'incidents dels sistemes d'informació, inclosos els específics de seguretat, que afecten la informació de CAC o als sistemes que la tracten.
- PSI-SI-07 CÒPIES DE RESPATLER I RECUPERACIÓ. Descriu la metodologia que s'ha de seguir per a la realització de còpies de respatler i la restauració de les mateixes.
- PSI-SI-08 IDENTIFICACIÓ I AUTENTICACIÓ D'USUARIS. Descriu la metodologia que s'ha de seguir per a dur a terme la identificació i l'autenticació dels usuaris en l'entorn de treball de CAC.
- PSI-SI-09 CONTROL D'ACCÉS LÒGIC. Definix les normatives i línies de treball aplicables per a dur a terme de forma satisfactòria el control d'accessos als recursos d'informació corporatius de CAC.
- PSI-SI-11 CONTROL DEL DISSENY D'APLICACIONS. Especifica les mesures de control associades al disseny i desenrotllament d'aplicacions orientades a Internet desenrotllades internament, així com a les modificacions posteriors per a garantir que es complix amb tots els requisits de seguretat.
- PSI-SI-13 CONTINUÏTAT DE LA SEGURETAT DE LA INFORMACIÓ. Definix els mecanismes necessaris per a reaccionar davant d'interrupcions severes dels sistemes informàtics i de comunicacions que afecten el negoci de Ciutat de les Arts i les Ciències a fi de protegir els seus sistemes d'informació i qualssevol altres actius enfront de grans fallades o desastres, així com de la prova, manteniment i avaluació de tals mecanismes.

- PSI-SI-14 GESTIÓ D'ÀREES SEGURES. Establix la sistemàtica per a la gestió de la seguretat física en els espais de la Ciutat de les Arts i les Ciències en què estan ubicats actius pertanyents al domini protegible
- PSI-SI-15 ANÀLISI DE RISCOS. Definix el procediment a aplicar per a la realització de l'Anàlisi de Riscos de Seguretat en CAC. Esta anàlisi té com a objecte la identificació i valoració d'amenaces, impactes i riscos que afecten els actius del domini protegible de l'organització.
- PSI-SI-16 CLASSIFICACIÓ I TRACTAMENT DE LA INFORMACIÓ. Descriu la classificació i el tractament de la informació corporativa dins de Ciutat de les Arts i les Ciències, per a garantir els nivells de seguretat apropiats durant la seua operació, emmagatzemament i trànsit
- PSI-SI-17 INTERCANVI D'INFORMACIÓ. Definix els models d'intercanvi d'informació en CAC, per a evitar la degradació dels subestats de seguretat de la informació en este procés.
- PSI-SI-18 GESTIÓ D'ACTIUS. Descriu els mecanismes d'operació necessaris per a garantir la seguretat en l'entrada i eixida d'actius de les àrees protegides de CAC.
- PSI-SI-19 GESTIÓ I CONTROL DE CANVIS DEL SISTEMA DE TICKETING. Definix la sistemàtica a seguir per a la gestió i el control dels canvis que comporten noves funcionalitats del sistema de Ticketing, o del programari utilitzat per al procés de vendes en la Ciutat de les Arts i les Ciències.
- PSI-SI-20 GESTIÓ DE MITJANS EXTRAÏBLES. Definix dels mecanismes de gestió dels mitjans extraïbles per a evitar danys als actius i la interrupció de les activitats de CAC.

La normativa de seguretat estarà a disposició de tots els membres de l'empresa, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible en la intraweb de l'empresa que es troba a disposició de tot el personal de l'empresa: http://intraweb.cac.es/politica_ens.pdf

11. OBLIGACIONS DEL PERSONAL

Tots els treballadors de CAC tenen l'obligació de conéixer i complir esta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comité de Gestió de la Seguretat de la Informació disposar dels mitjans necessaris perquè la informació arribe als afectats.

Tots els treballadors de la CIUTAT DE LES ARTS I LES CIÈNCIES assistiran a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per a atendre tot el personal de la CIUTAT DE LES ARTS I LES CIÈNCIES, en particular als de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessiten per a realitzar el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seua primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

12. TERCERES PARTS

Quan preste servicis a altres organismes o manege informació d'altres empreses, se'ls farà partícips d'esta Política de Seguretat de la Informació, s'establiran canals per a report i coordinació dels respectius Comités i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

Quan CIUTAT DE LES ARTS I LES CIÈNCIES utilitze servicis de tercers o cedisca informació a tercers, se'ls farà partícips d'esta Política de Seguretat i de la Normativa de Seguretat relacionada amb els dits servicis o informació. L'esmentada tercera part quedarà subjecta a les obligacions establides en aquesta normativa, podent desenrotllar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de report i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establit en esta Política.

Quan algun aspecte de la Política no puga ser satisfet per una tercera part segons es requerix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precise els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'este informe pels responsables de la informació i els servicis afectats abans de seguir avant.

Direcció General
Ciutat de les Arts i les Ciències