COSTAISA GROUP

Política de Seguretat

25/06/2018

Revisions

Revisiones				
Estat	**Revisió**	**Descripció del Canvi**	**Autors**	**Data efectiva**
Publicat	0	Publicació inicial	Antonio Serra Francisco Araújo	15/06/2018

ÍNDEX

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 15 de juny de 2018 per la Direcció General i el Comitè de Seguretat. Aquesta Política de Seguretat de la Informació és efectiva des d'aquesta data i fins que sigui reemplaçada per una nova Política. Aquest text anul·la l'anterior, que va ser aprovat el dia 30 de juny de 2011 per la Direcció.

2. INTRODUCCIÓN

Costaisa Group depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per 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 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 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, ús previst i valor de la informació i els serveis. 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 garantir la continuïtat dels serveis prestats.

Els diferents departaments han de cerciorar-se 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 a la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes TIC.

Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord a l'Article 7 del ENS.

3. PREVENCIÓ

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per a això els departaments han 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 garantir el compliment de la política, els departaments han de:

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

4. 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 en els nivells de prestació dels serveis i actuar en conseqüència segons l'establert 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 report que arribin als

responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

5. RESPOSTA

Els departaments han de:

1. Establir mecanismes per respondre eficaçment als incidents de seguretat.
2. Designar punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes.
3. 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).

6. 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 activitats de recuperació.

7. ABAST

Aquesta política s'aplica a tots els sistemes TIC de Costaisa Group i a tots els membres de l'organització, sense excepcions.

Referent a la ISO27001, l'abast del SGSI abasta els processos subjacents a l'àrea d'Explotació centrant-se en alguns dels processos més importants amb els quals ofereixen serveis als seus clients: Servei de Chaman, Gestió administrativa dels clients, Servei d'Intranet, Servei de correu electrònic, Servei d'emmagatzematge i manteniment de la web pública, Servei SIP (Sistema Integrat de Prevenció), Servei d'Escriptori de l'Usuari, Gestió de Nòmines i Personal dels Clients i els serveis de Hosting per a Sistemes SAP

8. MISIÓ, VISIÓ i VALORS

8.1 Misió

Costaisa Group pretén desenvolupar un negoci de continuïtat per contribuir a millorar el teixit industrial i productiu.

- Mitjançant la consultoria organitzativa i tecnològica ajuda a les empreses clients a aconseguir major èxit en el seu negoci.
- Garanteix la contractació de professionals amb qualitat d'ocupació i continuïtat en el lloc de treball.
- Proporciona beneficis als seus accionistes.
- Contribueix a millorar el teixit industrial mitjançant el disseny, desenvolupament i implantació de solucions organitzatives i tecnològiques.

8.2 Visió

Costaisa Group pretén convertir-se en la consultora de referència en els àmbits en els quals opera, i vol que els seus clients la considerin el seu soci organitzatiu i tecnològic per als seus projectes estratègics de negoci.

8.3 Valores

- Proximitat i confiança: el seu principal valor són els professionals que formen els equips de treball juntament amb els seus clients exercint una consultoria de proximitat i afermant relacions de confiança.
- Voluntat de millorar dia a dia: la competitivitat es guanya treballant cap a la millora contínua, per aquest motiu ha creat un Sistema de Gestió de la Qualitat per ajustar els nostres processos a les exigències del mercat.
- Actitud de desafiament: la meta és aconseguir els objectius dels seus clients.

9. MARC NORMATIU

9.1 Sistemas de Informació

9.1.1 Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter Personal

Responsable: Departament de seguretat
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.2 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 i pel qual es deroga la Directiva 95/46/CE

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.3 L 34/2002 d'11 Jul. (Serveis de la societat de la informació i de comerç electrònic)

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.4 Llei 9/2014, de 9 de maig, de Telecomunicacions.

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.5 OM PRE/2740/2007 de 19 Set. (Reglament d'Avaluació i Certificació de la Seguretat de les Tecnologies de la Informació)

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.6 Esquema Nacional de Seguretat

• Reial decret 951/2015, de 23 d'octubre, de modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.
• Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.
Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.7 Norma ISO27001 de Seguretat en els Sistemes d'Informació

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.8 Norma ISO20000 de Gestió de Serveis TU

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.1.9 Norma ISO22301 de Continuïtat de negoci

Responsable: Direcció Tècnica
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.2 Propietat Intel·lectual

9.2.1 Reial decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de Propietat Intel·lectual.

Responsable: Administració
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.3 Recursos Humans

9.3.1 Reial decret Legislatiu 2/2015, de 23 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut dels Treballadors

Responsable: Recursos Humans
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.3.2 Llei 3/2012, de 6 de juliol, de mesures urgents per a la reforma del mercat laboral

Responsable: Recursos Humans
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.3.3 Conveni col·lectiu d'Oficines i Despatxos

Responsable: Recursos Humans
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

9.3.4 Llei de Prevenció de Riscos Laborals (Llei 31/1995, de 8 de novembre).

Responsable: Recursos Humans
Assessor Legal: Brugueras, García-Bragado, Molinero & Associats

10. PROCEDIMENTS DE DESIGNACIÓ

La relació completa de comitès i funcions es pot trobar en la Normativa de Seguretat. El Responsable de Seguretat de la Informació serà nomenat per la Direcció a proposta del Comitè de Seguretat. El nomenament es revisarà cada 2 anys o quan el lloc quedi vacant.
El Departament responsable d'un servei que es presti electrònicament d'acord a la Llei 11/2007 designarà al Responsable del Sistema, precisant les seves funcions i responsabilitats dins del marc establert per aquesta Política.

11. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Serà missió del Comitè de seguretat 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 Comitè de Seguretat i difosa perquè la coneguin totes les parts afectades.

12. DADES DE CARÀCTER PERSONAL

Costaisa Group tracta dades de caràcter personal. El Document de Seguretat, al que tindran accés només les persones autoritzades, recull els fitxers afectats i els responsables corresponents. Tots els sistemes d'informació de Costaisa Group s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollits en l'esmentat Document de Seguretat.

13. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà regularment, almenys una vegada a l'any o quan:
1. Canviï la informació manejada
2. Canviïn els serveis prestats
3. Ocorri un incident greu de seguretat
4. Es reportin vulnerabilitats greus

Per a l'harmonització de les anàlisis de riscos, el Comitè de seguretat establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats. El Comitè de seguretat dinamitzarà la disponibilitat de recursos per atendre a les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

14. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta Política de Seguretat de la Informació complementa les polítiques de seguretat de Costaisa Group en diferents matèries:

- ISO27001 Seguretat de la Informació
- Esquema Nacional de Seguretat (ENS) (En procés de certificació)
- ISO22301 Continuïtat de Negoci (En procés de certificació)
- ISO20000 Gestió de Serveis TU (En procés de certificació)
- Reglament General de Protecció de Dades (RGPD)

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que afronti aspectes específics. La Normativa de Seguretat estarà a la disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per a aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions. La documentació estarà disponible en la BBDD Notes d'Instruccions i Manuals.

15. OBLIGACIONS DEL PERSONAL

Tots els membres de Costaisa Group tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de seguretat disposar els mitjans necessaris perquè la informació arribi als afectats.
Tots els membres de Costaisa Group atendran a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada a l'any. S'establirà un programa de conscienciació contínua

per atendre a tots els membres, 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 en què la necessitin per realitzar el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

16. TERCERES PARTS

Quan Costaisa Group presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals para reporti i coordinació dels respectius Comitès de Seguretat TIC s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.
Quan Costaisa Group utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que concerneixi a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per 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'establert en aquesta Política.
Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.