COSTAISA GROUP

Politique de sécurité

11/07/2019

Revisiones

Revisiones				
Estado	**Revisión**	**Descripción del Cambio**	**Autores**	**Fecha efectiva**
Publié	0	Publication initiale	Antonio Serra	15/06/2018
Publié	1	Mise à jour des éléments de la norme ISO22301, modifications mineures.	Antonio Serra	22/01/2019
Publié	2	• Les exigences de sécurité minimales liées à l'article 11 du Décret Royal 3/2010 sont ajoutées. • La référence aux services concernés par le plan de continuité est ajoutée. • La référence au LOPDPGDD est ajoutée et la référence au LOPD est supprimée.	Antonio Serra	16/05/2019

SOMMAIRE

1. APPROBATION ET ENTRÉE EN VIGUEUR

Texte approuvé le 15 juin 2018 par la direction générale et le comité de sécurité. Cette politique de sécurité des informations prendra effet à cette date et jusqu'à ce qu'elle soit remplacée par une nouvelle politique. Ce texte annule le texte précédent, qui avait été approuvé le 30 juin 2011 par la direction.

2. INTRODUCTION

Costaisa Group dépend des systèmes TIC (Technologies de l'Information et de la Communication) pour atteindre ses objectifs. Ces systèmes doivent être administrés avec diligence, en prenant les mesures appropriées pour les protéger contre des dommages accidentels ou délibérés qui pourraient nuire à la disponibilité, à l'intégrité ou à la confidentialité des informations traitées ou des services fournis.

L'objectif de la sécurité des informations est de garantir la qualité des informations et la fourniture continue des services, en agissant avec prévention, en supervisant les activités quotidiennes et en réagissant rapidement aux incidents. Les systèmes TIC doivent être protégés contre les menaces à évolution rapide qui pourraient nuire à la confidentialité, à l'intégrité, à la disponibilité, à l'usage prévu et à la valeur des informations et des services. Pour se défendre face à ces menaces, il faut une stratégie adaptée aux changements des conditions de l'environnement afin de garantir la prestation des services en continu. Cela implique que les départements doivent appliquer des mesures minimales de sécurité exigées par le Système National de Sécurité (ENS), mais également réaliser un suivi continu des niveaux de prestation des services, suivre et analyser les vulnérabilités signalées, et préparer une réponse efficace aux incidents afin de garantir que les services sont fournis en continu.

Les différents départements doivent s'assurer que la sécurité TIC est une partie intégrale de chaque étape du cycle de vie du système, de sa conception à son retrait du service, en passant par les décisions de développement ou d'acquisition et les activités d'exploitation. Les exigences de sécurité et les besoins de financement doivent être identifiés et inclus dans la planification, dans la demande d'offres, et dans les appels d'offres pour les projets de TIC.

Les départements doivent être préparés pour prévenir, détecter, réagir et se redresser après des incidents, conformément à l'article 7 de l'ENS.

3. PRÉVENTION

Dans la mesure du possible, les départements doivent éviter, ou au moins prévenir, que les informations ou les services soient affectés par des incidents de sécurité. Pour cela, les départements doivent mettre en œuvre les mesures minimales de sécurité déterminées par l'ENS, ainsi que tout autre contrôle supplémentaire identifié par le biais d'une évaluation des menaces et des risques. Ces contrôles, ainsi que les rôles et responsabilités de sécurité de l'ensemble du personnel, doivent être clairement définis et documentés.

Pour garantir le respect de la politique, les départements doivent:

1. Autoriser les systèmes avant d'entrer en opération.
2. Évaluer régulièrement la sécurité, y compris les évaluations de routine des modifications de configuration.
3. Demander la révision périodique par des tiers afin d'obtenir une évaluation indépendante.

4. DÉTECTION

Étant donné que les services peuvent se dégrader rapidement suite à des incidents, allant d'un simple ralentissement à un arrêt complet, les services doivent surveiller le fonctionnement en continu afin de détecter des anomalies dans les niveaux de prestation des services et agir en conséquence selon les dispositions établies dans l'article 9 de l'ENS.

La surveillance est particulièrement importante lorsque des lignes de défense sont établies conformément à l'article 8 de l'ENS. Il faudra établir des mécanismes de détection,

d'analyse et de rapport qui seront envoyés aux responsables régulièrement, et lorsqu'une différence importante sera observée par rapport aux paramètres normaux préétablis.

5. RÉPONSE

Les départements doivent:

1. Établir des mécanismes pour répondre efficacement aux incidents de sécurité.
2. Désigner un point de contact pour les communications relatives à des incidents détectés dans d'autres départements ou d'autres organismes.
3. Établir des protocoles pour l'échange d'informations en lien avec l'incident. Cela inclut des communications, dans les deux sens, formulées avec les Équipements de Réponse aux Urgences (CERT).

6. RETOUR À LA NORMALE

Pour garantir la disponibilité des services importants, les départements doivent développer des plans de continuité des systèmes TIC dans une partie de leur plan général de continuité commerciale et des activités de retour à la normale.

7. ÉTENDUE

Cette politique s'applique à tous les systèmes TIC de Costaisa Group et à tous les membres de l'organisation, sans exception.

En ce qui concerne la norme ISO27001, l'étendue du SGSI comprend les processus sous- jacents dans le domaine de l'exploitation qui sont centrés sur certains des processus les plus importants à l'aide desquels nous fournissons nos services à nos clients : Service de Chaman, Gestion administrative des clients, Service Intranet, Service e-mail, Service de stockage et de conservation du site web public, Service SIP (Système Intégré de Prévention), Service de Bureau de l'Usager, Gestion des Fiches de Paie et du Personnel des clients et services de Hosting pour les Systèmes SAP.

8. MISSION, VISION ET VALEURS

8.1 Mission

Costaisa Group a pour objectif de développer une activité en continu afin de contribuer à l'amélioration du réseau industriel et productif.

- Par le biais de la consultation organisationnelle et technologique, il aide les entreprises clientes à obtenir de meilleures performances.
- Il garantit l'embauche de professionnels de qualité qui garantissent une continuité sur leur poste de travail.
- Il fournit des bénéfices aux actionnaires.
- Il contribue à l'amélioration du réseau industriel grâce à la conception, au développement et à la mise en place de solutions organisationnelles et technologiques.

8.2 Vision

Costaisa Group a pour objectif de devenir le consultant de référence dans ses domaines d'activité, et souhaite que ses clients le considèrent comme leur partenaire organisationnel et technologique pour leurs projets stratégiques.

8.3 Valeurs

- Proximité et confiance: sa principale valeur, ce sont les professionnels qui forment les équipes de travail avec ses clients, qui exercent une consultation de proximité et entretiennent des relations de confiance.
- La volonté d'améliorer le quotidien: on devient compétitif en travaillant pour s'améliorer constamment, c'est pour cela que nous avons créé un Système de Gestion de la Qualité pour ajuster nos processus aux exigences du marché.
- Envie de relever des défis: l'objectif est d'atteindre les objectifs fixés par les clients.

9. CADRE RÉGLEMENTAIRE

9.1 Systèmes d'information

9.1.1 Loi organique 3/2018, du 5 décembre, de protection des données personnelles et garantie des droits numériques

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.2 Règlement (UE) 2016/679 du Parlement Européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques dans tous les aspects liés au traitement des données personnelles, à la libre circulation de ces données et qui abroge la Directive 95/46/CE

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.3 L 34/2002 du 11 juil. (Services de la société de l'information et du commerce électronique)

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.4 Loi 9/2014, du 9 mai, sur les télécommunications

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.5 OM PRE/2740/2007 du 19 sep. (Règlement de l'évaluation et de la certification de la sécurité des technologies de l'information)

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.6 Système National de Sécurité

- Décret Royal 951/2015, du 23 octobre, sur la modification du Décret Royal 3/2010, du 8 janvier, qui réglemente le Système National de Sécurité dans le secteur de l'administration électronique.

- Décret Royal 3/2010 du 8 janvier, qui réglemente le Système National de Sécurité dans le secteur de l'administration électronique.

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.7 Norme ISO27001 sur la sécurité dans les systèmes d'information

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.8 Norme ISO20000 sur la gestion des services TI

Responsable: Direction technique
Conseiller légal: Across Legal

9.1.9 Norme ISO22301 sur la continuité des opérations

Responsable: Direction technique
Conseiller légal: Across Legal

9.2 Propriété intellectuelle

9.2.1 Décret Royal législatif 1/1996, du 12 avril, qui approuve le texte consolidé de la loi sur la propriété intellectuelle

Responsable: Administration
Conseiller légal: Brugueras, García-Bragado, Molinero & Asociados

9.3 Ressources humaines

9.3.1 Décret Royal législatif 2/2015, du 23 octobre, qui approuve le texte consolidé de la loi sur le statut des travailleurs

Responsable: Ressources humaines
Conseiller légal: Brugueras, García-Bragado, Molinero & Asociados

9.3.2 Loi 3/2012, du 6 juillet, sur les mesures urgentes pour la réforme du marché du travail

Responsable: Ressources humaines
Conseiller légal: Brugueras, García-Bragado, Molinero & Asociados

9.3.3 Accord collectif des bureaux

Responsable: Ressources humaines
Conseiller légal: Brugueras, García-Bragado, Molinero & Asociados

9.3.4 Loi sur la prévention des risques au travail (Loi 31/1995, du 8 novembre)

Responsable: Ressources humaines
Conseiller légal: Brugueras, García-Bragado, Molinero & Asociados

10. PROCÉDURES DE DÉSIGNATION

Les relations complètes des comités et les postes peuvent être consultées dans la réglementation de sécurité. Le responsable de la sécurité des informations sera nommé par la direction sur proposition du comité de sécurité. La nomination sera révisée tous les 2 ans ou quand le poste sera vacant.
Le service responsable d'un service fourni de manière électronique conformément à la loi 11/2007 désignera le responsable du système, en précisant ses fonctions et responsabilités dans le cadre établi par cette politique.

11. POLITIQUE DE SÉCURITÉ DES INFORMATIONS

Le comité de sécurité aura pour mission la révision annuelle de cette politique de sécurité des informations et la proposition de révision ou de mise à jour de celle-ci. La politique sera approuvée par le comité de sécurité et fournie à toutes les parties concernées pour qu'elles puissent en prendre connaissance.

12. DONNÉES À CARACTÈRE PERSONNEL

Costaisa Group traite des données à caractère personnel. Le document de sécurité, auquel seules les personnes autorisées auront accès, recueille les fichiers concernés et les responsables correspondants. Tous les systèmes d'information de Costaisa Group seront paramétrés en fonction des niveaux de sécurité exigés par la réglementation pour la nature et la finalité des données à caractère personnel collectées dans le document de sécurité mentionné.

13. GESTION DES RISQUES

Tous les systèmes concernés par cette politique devront réaliser une analyse de risques évaluant les menaces et risques auxquels ils sont exposés. Cette analyse sera répétée régulièrement, au moins une fois par an ou lorsque:

1. Les informations sont modifiées
2. Les services fournis changent
3. Un grave incident de sécurité se produit
4. Des vulnérabilités graves sont signalées

Pour harmoniser les analyses des risques, le comité de sécurité établira une évaluation de référence pour les différents types d'informations traités et les différents services fournis. Le comité de sécurité stimulera la disponibilité des ressources pour répondre aux besoins de sécurité des différents systèmes, en promouvant les investissements de nature horizontale.

14. DÉVELOPPEMENT DE LA POLITIQUE DE SÉCURITÉ DES INFORMATIONS

Cette politique de sécurité des informations complète les politiques de sécurité du groupe Costaisa dans différents domaines:

- Sécurité de l'information ISO27001
- Système de Sécurité Nationale (SSN) (en cours de certification)
- Continuité de l'activité ISO22301 (en cours de certification)
- Gestion des services informatiques ISO20000 (en cours de certification)
- Réglementation générale sur la protection des données (RGPD)

Cette politique sera développée par le biais de règlements de sécurité qui traitent d'aspects spécifiques. La politique de sécurité sera disponible pour tous les membres de l'organisation qui en ont besoin, en particulier pour ceux qui utilisent, exploitent ou gèrent les systèmes d'information et de communication. La documentation sera disponible dans les notes d'instructions et les manuels de BBDD.

Les principes de base sont les suivants:

a) Organisation et mise en œuvre du processus de sécurité.
Il sera développé dans le règlement de sécurité actuel publié dans Instman.

b) Analyse et gestion des risques.
Il sera développé dans l'analyse de risque réalisée chaque année pour examen par la direction de l'ISMS. La méthodologie appliquée est expliquée dans l'instruction.

c) Gestion du personnel.
Il sera développé dans le règlement de sécurité actuel publié dans Instman.

d) Professionnalisme
Il sera développé dans le Règlement de sécurité actuel publié dans Instman et dans les manuels des fonctions pertinentes de chaque domaine / département.

e) Autorisation et contrôle d'accès.
Il sera développé dans le règlement de sécurité actuel publié dans Instman.

f) Protection des installations.
Il sera développé dans le règlement de sécurité actuel publié dans Instman.

g) Acquisition de produits.
Il est développé dans le manuel CS_MNPR_Procedure d'acquisition de composants.

h) Sécurité par défaut.
Il est inclus dans les différents manuels de Bastionado de Sistemas et dans le règlement de sécurité.

i) Intégrité et mise à jour du système.
Il est inclus dans le manuel SIMNPR01_20180219_QVM_Remediación_Vulnerabilidades et dans les différents manuels et procédures de Sistemas.

j) Protection des informations stockées et en transit.
Il sera développé dans le règlement de sécurité actuel publié dans Instman. Lorsque vous traitez des informations relatives à la santé des personnes, elles seront toujours cryptées, conformément aux manuels d'exploitation et de systèmes correspondants.

k) Prévention d'autres systèmes d'information interconnectés.
Il sera géré en suivant les manuels du système

l) Enregistrement d'activité.
L'outil d'entreprise QRadar collecte et gère tous les enregistrements, conformément aux manuels des systèmes correspondants.

m) Incidents de sécurité.
Il sera développé dans le règlement de sécurité actuel publié dans Instman.

n) Continuité de l'activité.
Il sera développé dans le plan de continuité, ME_MNPR_BIA d'analyse d'impact sur les entreprises et dans le règlement de sécurité actuel publié dans Instman. Vous trouverez la liste des services inclus dans le champ d'application de la liste des services pouvant être gérés par la continuité de l'activité de l'organisation dans le manuel M-2198 CS_MNPR_AlcanceSGSI / SGCN.

o) Amélioration continue du processus de sécurité.
Dans le cadre de l'ISMS et du SGCN, le système est examiné dans son intégralité au moins une fois par an à la suite du cycle de Deming (planifier, exécuter, vérifier, agir).

15. OBLIGATIONS DU PERSONNEL

Tous les membres de Costaisa Group ont l'obligation de connaître et de respecter cette politique de sécurité des informations et la réglementation de sécurité, le comité de sécurité ayant la responsabilité de disposer des moyens nécessaires pour que les informations soient transmises aux personnes concernées.
Tous les membres de Costaisa Group assisteront à une session de sensibilisation en matière de sécurité TIC au moins une fois par an. On établira un programme de sensibilisation continu pour prendre en charge tous les membres, en particulier les membres qui viennent d'arriver.
Les personnes ayant une responsabilité d'utilisation ou de contrôle des systèmes TIC recevront une formation afin de les utiliser de manière sécurisée dans la mesure du possible selon leur travail. La formation sera obligatoire avant d'assumer toute responsabilité, qu'il s'agisse de la première affectation ou d'un changement de poste de travail ou de responsabilités sur ce système.

16. TIERS

Lorsque Costaisa Group fournit ses services à d'autres organismes ou traite les informations d'autres organismes, ceux-ci seront inclus dans cette politique de sécurité des informations, on établira des canaux pour la rédaction de rapports et la coordination des comités de sécurité TIC respectifs, on établira des procédures d'action pour réagir à des incidents de sécurité.
Lorsque Costaisa Group contracte des services de tiers ou divulgue des informations à des tiers, ceux-ci seront inclus dans cette politique de sécurité et dans la réglementation de sécurité relative à ces services ou informations. Ces tiers seront sujets aux obligations établies dans la réglementation, et ils pourront développer leurs propres procédures opératives pour s'y conformer. On établira des procédures spécifiques pour les rapports et la résolution d'incidents. On assurera que le personnel des tiers est correctement sensibilisé en matière de sécurité, au moins au même niveau que celui établi dans cette politique.
Lorsqu'un aspect de la politique ne peut pas être respecté par un tiers selon les exigences des paragraphes précédents, on exigera un rapport du responsable de la sécurité qui signalera les risques encourus et la manière de les prévenir. L'approbation de ce rapport sera requise par les responsables de l'information et des services concernés avant de procéder.

Le suivi du service des fournisseurs est traité dans le CS_MNPR_Procedimiento du suivi des SLA avec des fournisseurs.