POLITIQUE DE SÉCURITÉ DE L'INFORMATION

1.INTRODUCTION

La Politique de Sécurité de l'Information est élaborée conformément à l'exigence du Décret Royal 3/2010 du 8 janvier qui réglemente le Système de Sécurité National dans le domaine de l'Administration Électronique, qui établit à son article 11: l'obligation pour les Administrations Publiques de disposer d'une Politique de Sécurité et indique les exigences minimales à respecter.

Cette Politique de Sécurité suit également les indications du guide CCN-STIC-805 du Centre National de Cryptologie, centre rattaché au Centre National de Renseignement.

Le Système de Sécurité National a pour objectif la création des conditions nécessaires de confiance dans l'utilisation des moyens électroniques, grâce à des mesures visant à garantir la sécurité des systèmes, des données, des communications et des services électroniques, ce qui accorde aux citoyens et aux administrations publiques, l'exercice des droits et permet l'accomplissement des devoirs par le biais de ces moyens.

L'Université d'Almería utilise les systèmes informatiques (TICE) pour atteindre ses objectifs institutionnels. Par conséquent, il s'avère nécessaire de garantir une gestion scrupuleuse de ces systèmes, en adoptant les mesures les mieux adaptées afin de les protéger contre tout dommage accidentel ou délibéré susceptible d'affecter la disponibilité, l'intégrité ou la confidentialité des informations traitées ou des services fournis.

Pour ces raisons, la sécurité de l'information a pour objectif de garantir la qualité de l'information et la continuité de la fourniture de services, en agissant de manière préventive, en surveillant les activités quotidiennes et en réagissant rapidement aux incidents.

Les systèmes TICE doivent être protégés contre les menaces à évolution rapide susceptibles d'affecter la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des informations et des services. Une stratégie de protection adaptée aux changements des conditions environnementales est donc nécessaire pour garantir la fourniture continue des services.

Cela implique, de la part de l'organisation et de son personnel, l'application des mesures de sécurité minimales requises par le Décret Royal 3/2012 (Système de Sécurité National), la surveillance en permanence des niveaux de prestation de services, la surveillance et

l'analyse des vulnérabilités signalées, la mise en place d'une action de réponse efficace aux incidents pour assurer la continuité des services fournis.

L'organisation est censée s'assurer que la sécurité informatique fait partie intégrante de chaque étape du cycle de vie du système, à partir de sa conception, à sa mise hors service, en passant par les décisions concernant le développement ou les investissements voire les activités d'exploitation.

Les exigences de sécurité et les besoins de financement doivent être identifiés et inclus dans la planification, la demande d'offre et les documents d'appel d'offres pour les projets TICE.

L'organisation doit être prête à prévenir, détecter, réagir et récupérer ses systèmes lors d'incidents, conformément à l'Article 7 de l'ENS.

1 .1.PRÉVENTION

L'organisation doit éviter, ou alors, tout au moins éviter autant que possible, que des informations ou des services soient endommagés par des incidents de sécurité. À cette fin, les mesures de sécurité minimales déterminées par l'ENS doivent être mises en œuvre, ainsi que tout contrôle supplémentaire identifié par le biais d'une évaluation des menaces et des risques.

Ces contrôles, ainsi que les rôles et responsabilités en matière de sécurité de tout le personnel, doivent être clairement définis et documentés. Pour assurer le respect de la politique de sécurité, l'organisation doit:

- Autoriser les systèmes avant leur mise en service.
- Évaluer régulièrement la sécurité, évaluer les modifications de configuration, effectuées régulièrement.
- Demander un contrôle périodique de la part des tiers, afin d'obtenir une évaluation indépendante.

1 .2.DÉTECTION

Etant donné que les services peuvent se dégrader rapidement en cas d'incidents, l'opération doit être surveillée en permanence afin de détecter toute anomalie dans les niveaux de fourniture des services et agir en conséquence, comme le prévoit l'Article 9 de la ENS.

Le contrôle est particulièrement important lorsque les lignes de défense sont établies conformément à l'Article 8 du ENS. Des mécanismes de détection, d'analyse et de rapport seront mis en place et remis aux responsables de façon régulière et en cas de divergence importante par rapport aux paramètres préétablis.

1 .3.RÉPONSE

L'organisation doit:

- Établir des mécanismes pour réagir efficacement face aux incidents de sécurité.
- Désigner un point de contact pour les communications relatives aux incidents détectés à l'intérieur de l'Istitution voire concernant d'autres organisations liées à la UAL.
- Établir des protocoles pour l'échange d'informations relatives à l'incident. Cela inclut les communications, dans les deux sens, avec les équipes d'intervention d'urgence reconnues au niveau national (CERT): Iris-CERT, CCN-CERT, ...

1 .4. PLAN DE REPRISE APRÈS INCIDENT

Pour garantir la disponibilité des services critiques, l'organisation doit élaborer des plans de continuité des systèmes informatiques dans le cadre de son plan général de continuité de service et des procédures de récupération.

2.MISSION

Conformément aux statuts en vigueur, l'Université d'Almeria est une institution de droit public, dotée de la personnalité juridique et dotée de ressources propres, assurant le service public de l'enseignement supérieur par le biais de l'enseignement, des études et de la recherche, en pleine autonomie et conformément à la Constitution et aux Lois.

Dans l'accomplissement de cette mission, l'organisation souligne la nécessité d'une infrastructure informatique qui priorise et encourage les opérations ouvertes, axées sur la fonctionnalité, la connectivité et le service aux utilisateurs, en tant que fonctions prioritaires pour la réalisation des objectifs stratégiques et institutionnels.

3. CHAMP D'APPLICATION

En raison de la mission de l'Institution, définie au point 3 de ce document, l'organisation rejette l'application de cette politique de sécurité à l'ensemble du système d'information.

Par conséquent, l'organisation appliquera cette politique de sécurité sur l'ensemble des systèmes informatiques qu'elle gère de manière centralisée via le Service des Technologies de l'Information et de la Communication, et plus précisémen, à tous les

systèmes liés à l'exercice des droits par voie électronique, au respect des obligations par voie électronique ou à l'accès à l'information voire aux procédures administratives.

Plus concrètement, cette politique de sécurité est applicable aux services suivants et aux systèmes informatiques qui les composent:

- Système ERP [1] Institutionnel:
  - Gestion Académique
  - Gestion Économique
  - Gestion des Ressources Humaines
  - Gestion de la Recherche
  - Gestion de la Qualité
  - Gestion des Espaces
  - Campus Virtuel

- **Système d'Administration Électronique:**
  - Administration Électronique
  - Service d'assistance aux utilisateurs

- **Système d' Enseignement Virtuel**

3 .1.Extension du champ d'application

De plus, et même en comprenant que les services suivants ne relèvent pas directement du domaine défini par le système de sécurité national, en raison de son importance à l'intérieur de la communauté universitaire, il est convenu d'étendre le champ d'application au service suivant de la UAL**:**

- **Système Web Institutionnel**

4.CADRE NORMATIF

Les lois et réglementations espagnoles relatives à la protection des données personnelles, à la propriété intellectuelle et à l'utilisation d'outils télématiques sont applicables. Pour toutes ces raisons, les organismes administratifs compétents peuvent exiger que les utilisateurs fournissent les enregistrements électroniques ou toute autre information liée à l'utilisation des systèmes d'information.

Cette politique s'inscrit dans le cadre juridique défini par les lois et Décrets Royaux suivants:

- Règlement Européen 2016/679 sur la Protection des Données, du Parlement Européen et du Conseil du 27 avril 2016, concernant la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données, et abrogeant la directive 95/46 / CE.
- Loi Organique des Universités (6/2001) et Loi Organique de modification de la LOU (4/2007).
- Loi 39/2015 du 1er octobre de la Procédure Administrative Commune des Administrations Publiques
- Loi 40/2015 du 1er octobre sur le régime juridique du secteur publique
- Système Nationale de la sécurité des systèmes d'information (Esquema Nacional de Seguridad) (DR 3/2010)
- Loi Organique sur la Protection des Données (15/1999) et Règlement de la Mise en oeuvre de la Loi Organique (DR 1720/2007)
- Loi sur les Services de la Société de l'information (du 12 octobre 2002)

5.ORGANISATION DE LA SÉCURITE

5.1. DÉLÉGUÉ DE LA PROTECTION DES DONNÉES (DPD)

Ce sera une personne ayant des connaissances spécialisées en Droit et en ce qui concerne les pratiques dans le domaine de la protection des données. Ces connaissances seront nécessaires en ce qui concerne les traitements, ainsi que les mesures à adopter pour garantir un traitement adéquat des données à caractère personnel.

Le Délégué à la Protection des Données doit exécuter ses tâches et ses fonctions en toute indépendance.

Les fonctions du Délégué sont spécifiées à l'article 39 de la *RGPD* , à savoir:

- Informer et conseiller tantôt le responsable ou le chargé du traitement tantôt les employés qui s'occupent du traitement des obligations de la RPDG voire des autres réglementations applicables en matière de protection des données.
- Superviser le respect de la RGPD et des autres réglementations applicables en matière de protection des données, ainsi que des politiques du responsable ou chargé du traitement de données, y compris l'attribution des responsabilités, la sensibilisation et la formation du personnel impliqué dans les opérations de traitement et les audits.
- Offrir le conseil demandé concernant l'évaluation d'impact en matière de protection des données et superviser son application conformément à l'article 35 de la RGPD.
- Coopérer avec l'autorité de contrôle.
- Agir en tant que point de contact de l'Autorité de contrôle en ce qui concerne les questions relatives au traitement, entre autres choses la consultation préalable de l'article 36 du RGPD, et réaliser des consultations, le cas échéant, sur toute autre question.

5.2 .COMITÉS: FONCTIONS ET RESPONSABILITÉS

Les fonctions du **Comité de Gestion de l'ENS** sont prises en charge par la **Commission sur la Sécurité de l'Information et la Protection des Données** , dénommée par la suite Commission de Sécurité.

La Commission de Sécurité est censée informer l'Équipe Présidentielle de l'Université.

Les fonctions de la Commission de Sécurité concernant l'ENS sont les suivantes:

- Diffusion de la politique et des règlements de sécurité de l'Institution.
- Approbation du règlement de écurité de l'Institution.
- Revue annuelle de la politique de sécurité.
- Développement de la procédure de désignation des rôles.
- Désignation des fonctions et des responsabilités.
- Supervision et approbation des tâches de suivi du Système de Sécurité National:
    - Tâches d'adéquation
    - Analyse des risques
    - Audit Biennal

5.3 .RÔLES: FONCTIONS ET RESPONSABILITÉS

.

Responsable de l'information

Le **Secrétariat Général** se chargera du rôle de responsable de l'information de l'Institution. Le Secrétariat Général est chargé des fonctions suivantes:

- Définition des exigences de l'information en matière de sécurité.
- Collaboration avec le responsable de la sécurité et avec le responsable du système dans le cadre de la maintenance des systèmes catalogués conformément à l'Annexe I du Système de sécurité national.

Responsable des services TICE

Le Gestionnaire (Gerente) de l'Université assumera le rôle de responsable des services informatiques de l'Institution avec les fonctions suivantes:

- Définition des exigences en services TIC en matière de sécurité.
- Collaboration avec le responsable de la sécurité, collaboration avec le responsable du système dans le cadre des activités de maintenance des systèmes catalogués conformément à l'annexe I du Système de Sécurité National.

Responsable de la Sécurité

Le Directeur du Service des Technologies de l'Information et de la Communication sera chargé de la fonction de responsable de la sécurité de l'Institution, selon les fonctions suivantes:

- Assurer la sécurité des informations traitées et des services fournis par les systèmes informatiques dans son domaine de responsabilité.
- Promouvoir la formation et la sensibilisation du Service des Technologies de l'Information et de la Communication dans les limites de son mandat.
- Vérification de conformité des mesures de sécurité établies pour la protection des informations traitées et des services fournis.
- Analyser, rédiger et approuver toute la documentation relative à la sécurité du système.
- Surveiller l'état de sécurité du système fourni par les outils de gestion des événements de sécurité et des mécanismes d'audit mis en œuvre à l'intérieur du système.
- Soutenir et superviser les enquêtes sur les incidents de sécurité, à partir de la notification jusqu'à la résolution.
- Rédiger le rapport périodique de sécurité informatique pour le propriétaire du système, avec prise en compte des incidents les plus importants de la période.
- Approuver des procédures de sécurité mises en place par le Responsable du Système.
- Élaborer le règlement de sécurité de l'Institution.

La figure de "Responsable de la Sécurité" définie par l'ENS ne coïncide pas avec la figure de responsable pour la sécurité des archives numériques de l'Univeristé.

Responsables du système informatique

Les chefs de service du Service des Technologies de l'Information et de la Communication sont désignés dans le rôle de Responsables du Système de l'Institution universitaire, ayant pour fonctions, dans leur domaines d'action, les actions suivantes:

- Développer, exploiter et maintenir le système tout au long de son cycle de vie, de ses spécifications, de son installation et vérification de son fonctionnement conforme.
- Définir la topologie et la politique de gestion du Système, en définissant les critères d'utilisation et les services disponibles.

- Définir la politique de connexion ou de déconnexion des dispositifs et des nouveaux utilisateurs du Système.
- Approuver les modifications concernant la sécurité du mode de fonctionnement du Système.
- Déterminer les mesures de sécurité qui seront appliquées par les fournisseurs de composants du Système au cours des étapes de développement, d'installation et de vérification.
- Mettre en œuvre et contrôler les mesures de sécurité spécifiques du Système et veiller sur leur intégration conforme dans le cadre général de la sécurité.
- Déterminer la configuration autorisé concernant le matériel et logiciels à utiliser dans le Système.
- Approuver toute modification substantielle de la configuration de tout élément du Système.
- Exécuter le processus obligatoire d'analyse et de gestion des risques dans le Système.
- Déterminer la catégorie du système conformément à la procédure décrite à l'Annexe I du ENS et déterminer les mesures de sécurité à appliquer décrites à l'Annexe II du ENS.
- Rédiger et approuver la documentation de sécurité du Système.
- Délimiter les responsabilités de chaque entité impliquée dans la maintenance, le fonctionnement, la mise en œuvre et la supervision du Système.
- *Assurer le respect des obligations de l'Administrateur de la Sécurité du Système (ASS).*
- Examiner les incidents de sécurité concernant le Système, à relater, le cas échéant, au Responsable de la Sécurité.
- Établir des plans de contingence et d'urgence avec mise en oeuvre de fréquents exercices pour garantir la familiarisation avec les plans et procédures de sûreté de la part du personnel.
- En outre, le responsable du système peut prévoir la suspension du traitement de certaines informations ou la fourniture d'un service donné en cas de graves problèmes de sécurité pouvant compromettre l'accomplissement des exigences établies. à condition que cette décision soit au préalable approuvée par les responsables des informations concernées, du service concerné et par le responsable de la sécurité.
- Élaboration des procédures de sécurité nécessaires pour l'opération dans le système.

<u>Administrateur de la Sécurité du Système</u>

L'administrateur des Services de Réseau et de la Sécurité TICE aura le rôle d'Administrateur de la Sécurité du Système ayant les fonctions suivantes:

- Vérifier l'approbation des procédures opérationnelles de sécurité
- Assurer le respect des contrôles de sécurité
- S'assurer que les procédures approuvées de gestion du système d'information sont appliquées
- Superviser les installations matérielles et logicielles, leurs modifications et améliorations pour garantir le respect des exigences de la sécurité en conformité aux autorisations appropriées.
- Vérifier la surveillance de l'état de la sécurité du système
- Informer les Responsables de la Sécurité et du Système de toute anomalie, compromission ou vulnérabilité concernant la sécurité
- Collaborer aux enquêtes et à la résolution des incidents de sécurité, à partir de la phase de la détection jusqu'à la résolution.

5.4 .POLITIQUE DE SÉCURITÉ

La Commission de sécurité aura pour mission de réviser chaque année la présente politique de Sécurité de l'Information et de proposer sa modification ou confirmation. La Politique de Sécurité sera approuvée par le Conseil de la Présidence Universitaire et diffusée afin que toutes les parties concernées en soient informées.

6.DONNÉES DE CARACTÈRE PERSONNEL

L'Université effectue des traitements dans lesquels des données à caractère personnel sont utilisées, en adoptant les mesures de sécurité appropriées conformément aux directives du Règlement Européen sur la Protection des Données, aux indications du Délégué à la Protection des Données en conformité au principe de responsabilité proactive et au principe de responsabilité établi par les normatives de sécurité en vigueur.

7. GESTION DES RISQUES

Tous les systèmes soumis à cette Politique doivent effectuer une analyse des risques, en évaluant les menaces et les risques auxquels ils sont exposés. Cette analyse sera répétée:

- Régulièrement, au moins une fois tous les deux ans
- Quand l'information traitée change
- Quand les services rendus changent
- Lorsqu'un incident de sécurité grave se produit
- Lorsque des vulnérabilités graves sont signalées
- Sous indication du Délégué à la Protection des Données.

Pour harmoniser l'analyse des risques, la Commission de Sécurité établira une évaluation de référence pour les différentes typologies d'informations traitées et les différents services fournis.

Le Comité de la Sécurité des TICE rationalisera la disponibilité des ressources pour répondre aux besoins de sécurité des différents systèmes, en favorisant les investissements horizontaux.

8. DÉVELOPPEMENT DE LA POLITIQUE DE SÉCURITÉ

Cette politique sera développée par le biais de réglementations de sécurité traitant des aspects spécifiques. Le règlement de sécurité sera mise à la disposition de tous les membres de l'Institution étant censés en prendre connaissance, en particulier de ceux qui utilisent, exploitent ou gèrent les systèmes d'information et de communication.

Le règlement de sécurité sera disponible sur l'intranet, via le portail d'administration électronique (http://ae.ual.es) et sur le site Web de la Commission de Sécurité (http://seguridad.ual.es).

Le règlement de sécurité format papier est disponible auprès du Service des Technologies de l'Information et de la Communication de l'Université.

9.OBLIGATIONS DU PERSONNEL

Tous les membres de l'Université ont l'obligation de connaître et de se conformer à la présente Politique de Sécurité de l'information et au règlement de sécurité qui en découle, la responsabilité incombant à la Commission de sécurité de mettre en place les moyens nécessaires pour que les informations parviennent aux personnes concernées. .

Tous les travailleurs de l'Université participeront à une action de sensibilisation à la sécurité des TICE au moins une fois tous les deux ans. Un programme continu d'actions de **sensibilisation** sera mis en place pour assister tous les membres de l'Université, en particulier les nouveaux membres, en tenant toujours compte de la disponibilité budgétaire.

Les personnes chargées de l'utilisation, de l'exploitation ou de l'administration de systèmes TIC recevront une formation sur la manipulation sans danger des systèmes, pour effectuer leur travail. La formation sera obligatoire avant d'assumer des responsabilités, qu'il s'agisse d'une première mission ou d'un changement de travail ou de responsabilités.

10.TIERCES PARTIES

Lorsque l'Université fournit des services à d'autres organisations ou gère des informations provenant d'autres organisations, celles-ci seront impliquées dans la présente Politique de Sécurité des informations .À cette fin, des voies de communication et de coordination des comités de coordination respectifs de l'ENS seront établies et des procédures d'action seront mises en place pour la réponse aux incidents de sécurité.

Lorsque l'Université utilise des services tiers ou transfère des informations à des tiers, ceux-ci seront impliqués dans la présente Politique de Sécurité et dans le règlement de sécurité concernant les services ou informations.Cette tierce partie sera soumise aux obligations énoncées dans les règlements susmentionnés et pourra élaborer ses propres procédures opérationnelles conformes. Des procédures spécifiques pour le signalement et la résolution des incidents seront établies.Le personnel tiers sera censé être formé en matière de sécurité, en conformité et dans le respect de la présente Politique de Sécurité. Lorsque certains aspects de cette Politique de Sécurité ne peuvent pas être satisfaits par une tierce partie, comme requis dans les paragraphes précédents, un rapport du responsable de la sécurité sera requis pour préciser les risques préviibles et la manière de les gérer.
Le rapport doit être approuvé par les responsables des informations et des services concernés avant poursuite.

11 ENTRÉE EN VIGUEUR

Cette Politique de Sécurité des Informations entre en vigueur le jour suivant sa date d'approbation par le Conseil d'Administration de l'Université et jusqu'à ce qu'elle soit remplacée par une nouvelle politique.

Est abrogée la précédente Politique de Sécurité des informations, approuvée par le Conseil de la Présidence de l'Université d'Almería le 17 décembre 2012.

1

[1] ERP = Système de planification des ressources d'entreprise.De l'anglais *Enterprise Resource Planning*