POLITICA DI SICUREZZA DELL'INFORMAZIONE

1.INTRODUZIONE

La Politica di Sicurezza dell'Informazione è stata elaborata in conformità con il regio decreto 3/2010, dell'8 gennaio, che disciplina il regime di sicurezza nazionale nel settore dell'Amministrazione Elettronica, che all'articolo 11 stabilisce l'obbligo per le Pubbliche Amministrazioni di adottare una politica di sicurezza indicandone i requisiti minimi che devono essere soddisfatti.

Tale Politica di Sicurezza segue altresí le indicazioni della guida CCN-STIC-805 del Centro Criptológico Nacional, facente capo al Centro Nazionale di Intelligence.

La finalità dello Schema Nazionale di Sicurezza é la creazione delle condizioni necessarie di sicurezza nell'uso dei mezzi elettronici, attraverso misure volte a garantire la sicurezza dei sistemi, dei dati, delle comunicazioni e dei servizi elettronici, che consenta ai cittadini e alle Amministrazioni Pubbliche, l'esercizio dei diritti e l'adempimento dei doveri attraverso tali mezzi.

L'Università di Almería si avvale di sistemi ICT (Tecnologie dell'Informazione e delle Comunicazioni) per il raggiungimento dei propri obiettivi istituzionali. Di conseguenza, corre l'obbligo di ricorrere ad una amministrazione scrupolosa di tali sistemi, adottando le misure appropriate per proteggerli da danni accidentali o deliberati che potrebbero compromettere la disponibilità, l'integrità o la riservatezza delle informazioni elaborate o dei servizi forniti.

Pertanto, l'obiettivo della Sicurezza delle Informazioni è garantire la qualità delle informazioni e la fornitura continua di servizi, agendo preventivamente, supervisionando l'attività quotidiana e reagendo prontamente agli incidenti.

I sistemi TIC devono essere protetti da minacce in rapida evoluzione, potenzialmente in grado di influenzare la riservatezza, l'integrità, la disponibilità, l'uso previsto e il valore delle informazioni e dei servizi. Per difendersi da queste minacce, è necessaria una strategia che si adatti ai cambiamenti delle condizioni ambientali per garantire la fornitura continua di servizi.

A ció consegue che l'organizzazione ed il personale siano tenuti ad applicare le misure minime di sicurezza richieste dal Regio Decreto 3/2012 (Schema Nazionale di Sicurezza), nonché a monitorare costantemente i livelli di fornitura del servizio, monitorare e

analizzare le vulnerabilità segnalate e preparare infine una risposta efficace agli incidenti per garantire la continuità dei servizi forniti.

L'organizzazione deve garantire che la sicurezza delle TIC sia parte integrante di ogni fase del ciclo di vita del sistema, dalla sua ideazione alla fase finale, attraverso decisioni di sviluppo o acquisizione e di impiego.

I requisiti di sicurezza e le esigenze di finanziamento devono essere identificati e inclusi nella pianificazione, nella richiesta di offerte e nei documenti di gara per i progetti TIC.

L'organizzazione deve essere preparata a prevenire, rilevare, reagire e recuperarsi dagli incidenti, in base all'articolo 7 dell'ENS.

1 .1.PREVENZIONE

L'organizzazione deve evitare, o almeno impedire, per quanto possibile, che le informazioni o i servizi si vedano pregiudicati da incidenti di sicurezza. A tal fine, devono essere implementate le misure minime di sicurezza stabilite dall'ENS come ogni ulteriore controllo addizionale identificato attraverso una valutazione delle minacce e dei rischi.

Tali controlli, cosí come i ruoli e le responsabilità in riferimento alla sicurezza di tutto il personale devono essere chiaramente definiti e documentati. Per garantire il rispetto della Politica di Sicurezza, l'organizzazione deve:

- Autorizzare i sistemi previamente alla loro entrata in funzione.
- Valutare costantemente la sicurezza, includendo le valutazioni delle modifiche di configurazione effettuate su base regolare.
- Richiedere una revisione periodica da parte di terzi al fine di ottenere una valutazione indipendente.

1 .2.RILEVAMENTO

Poiché i servizi possono degradarsi rapidamente a causa di incidenti, occorre provvedere ad un monitoraggio costante dell'operazione al fine di rilevare le possibili anomalie nei livelli di fornitura dei servizi e agire di conseguenza come stabilito nell'Articolo 9 dell'ENS.

Il monitoraggio è particolarmente rilevante quando siano stabilite le linee di difesa conformemente all'articolo 8 dell'ENS. Verranno stabiliti meccanismi di rilevamento, analisi e reporting che consentano l'identificazione dei responsabili con regolarità e quando si riscontri una deviazione significativa dai parametri prestabiliti.

1 .3.RISPOSTA

L'organizzazione deve:

- Stabilire meccanismi per rispondere efficacemente agli incidenti di sicurezza.
- Designare un punto di contatto per le comunicazioni relative agli incidenti rilevati in aree dell'Istituzione o in altre organizzazioni correlate alla UAL.
- Stabilire protocolli per lo scambio di informazioni relative all'incidente. Ciò include le comunicazioni, in entrambe le direzioni, con le Squadre di Intervento per le Emergenze (Equipos de Respuesta a Emergencias (CERT), riconosciute a livello nazionale: Iris-CERT, CCN-CERT, ...

1 .4.RECUPERO

Per garantire la disponibilità dei servizi critici, l'organizzazione deve sviluppare piani di continuità per i sistemi TIC come parte del suo piano generale per le attività di business continuity e recovery.

2.MISSIONE

Come risulta dai suoi statuti, attualmente in vigore, l'Università di Almeria è un'istituzione di diritto pubblico, dotata di personalità giuridica e beni propri, la cui missione si esplica nel servizio pubblico di istruzione superiore attraverso l'insegnamento, lo studio e la ricerca, con piena autonomia e in conformità con la Costituzione e le leggi.

In stretta correlazione con l'adempimento di tale missione, l'organizzazione tiene a manifestare la necessità di un'infrastruttura TIC che privilegi e incoraggi le operazioni aperte, incentrate sulla funzionalità, la connettività e il servizio all'utente, come funzioni prioritarie per il raggiungimento degli obiettivi strategici. e istituzionali.

3.AMBITO

in ottemperanza alla sua missione, cosi come riportato al punto 3 di questo documento, l'organizzazione ravvisa l'inapplicabilità di questa politica di sicurezza sull'intero sistema informativo.

Ció premettendo, l'organizzazione applicherà questa politica alla maggior parte dei sistemi TIC che gestisce a livello centrale attraverso il Servizio di Tecnologia dell'Informazione e della Comunicazione, e in particolare su tutti quei sistemi correlati all'esercizio dei diritti. con mezzi elettronici, con l'adempimento dei doveri mediante mezzi elettronici o con l'accesso alle informazioni o alle procedure amministrative..

In termini concreti, questa politica di sicurezza è applicabile ai seguenti servizi e ai sistemi TIC che li compongono:

- **Sistema ERP [1] Istituzionale:**
  - Gestione Accademica
  - Gestione Economica
  - Gestione delle Risorse Umane
  - Gestione della Ricerca
  - Gestione della Qualità
  - Gestione degli Spazi
  - Campus Virtuale

- **Sistema di Amministrazione Elettronica:**
  - Amministrazione Elettronica
  - Servizio agli Utenti

- **Sistema di Insegnamento Virtuale**

3 .1.Estensione dell'ambito

Inoltre, pur comprendendo che i seguenti servizi non sono direttamente inclusi nel campo di applicazione dello Schema Nazionale di Sicurezza, a causa della sua importanza nella comunità universitaria, si accetta di estendere l'ambito al seguente servizio della UAL:

- **Sistema Web Istituzionale**

4.QUADRO NORMATIVO

Sono applicabili le leggi e le normative spagnole relative alla protezione dei dati personali, della proprietà intellettuale e all'uso di strumenti telematici. Per tutti questi motivi, la UAL potrebbe richiedere agli organi amministrativi competenti di fornire i record elettronici o qualsiasi altra informazione relativa all'utilizzo dei sistemi di informazione.

Questa politica si situa all'interno del quadro giuridico definito dalle seguenti leggi e Reali Decreti:

- Regolamento Europeo sulla Protezione dei Dati 2016/679, del Parlamento Europeo e del Consiglio d'Europa, del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione dei dati, e che abroga la direttiva 95/46 / CE.

- Legge Organica delle Università (6/2001) e Legge Organica di modifica della L.O.U.(4/2007).
- Legge 39/2015 del 1 ° ottobre della Procedura Amministrativa Comune delle Pubbliche Amministrazioni
- Legge 40/2015 del 1 ° ottobre sul regime giuridico del settore pubblico
- Schema di Sicurezza Nazionale (RD 3/2010)
- Legge Organica sulla Protezione dei Dati (15/1999) e Regolamento per lo sviluppo della Legge Organica (RD 1720/2007)
- Legge dei Servizi della Società dell'Informazione (del 12 ottobre 2002)

5.ORGANIZZAZIONE DELLA SICUREZZA

5.1. DELEGATO PER LA PROTEZIONE DEI DATI (DPD)

Sarà una persona con conoscenze specializzate nel Diritto e nella pratica nel campo della protezione dei dati. Tali conoscenze saranno richieste in relazione ai trattamenti che vengono realizzati, nonché alle misure che devono essere adottate per garantire l'adeguatezza del trattamento dei dati personali.

Il Delegato per la Protezione dei Dati deve svolgere i propri compiti e le proprie funzioni in totale indipendenza.

Le funzioni del Delegato sono specificate nell'articolo 39 del *RGPD* , sono le seguenti:

- Informare e prestare consulenza al responsabile o agli adetti al trattamento trattamento degli obblighi del RPGD e ulteriori normative applicabili in materia di protezione dei dati.
- Supervisionare l'applicazione conforme del RGPD e delle altre normative applicabili alla protezione dei dati e delle politiche relative al responsabile o addetto al trattamento di tali dati, includendo l'assegnazione delle responsabilità, la consapevolezza e la formazione del personale coinvolto nelle operazioni di trattamento e gli audit corrispondenti.
- Fornire il proprio parere sulla valutazione dell'impatto relativo alla protezione dei dati e supervisionare la sua applicazione conforme all'articolo 35 del RGPD.
- Cooperare con l'Autorità di controllo.
- Agire come punto di contatto dell'Autorità di controllo per le questioni relative al trattamento, compresa la previa consultazione dell'articolo 36 del RGPD, e prestare consulenza su qualsiasi altra questione.

5.2 .COMITATI: FUNZIONI E RESPONSABILITÀ

Le funzioni del **Comitato di gestione dell'ENS** sono assunte dall'attuale **Commissione per la Sicurezza Informatica e la Protezione dei Dati** , in appresso "Commissione per la Sicurezza".

La Commissione per la Sicurezza terrà informata la Governance dell'Università.

Le funzioni della Commissione per la Sicurezza in relazione all'ENS sono:

- Diffusione della politica e dei regolamenti di sicurezza dell'Organizzazione.
- Approvazione delle norme di sicurezza dell'Organizzazione.
- Revisione annuale della politica di sicurezza.
- Sviluppo della procedura per la designazione dei ruoli.
- Designazione di ruoli e responsabilità.
- Supervisione e approvazione dei compiti di follow-up dello Schema di Sicurezza Nazionale:
    - Compiti di adeguamento
    - Analisi del Rischio
    - Audit Biennale

5.3 .RUOLI: FUNZIONI E RESPONSABILITÀ

.

Responsabile dell'informazione

La **Segreteria Generale** avrà il ruolo di responsabile delle informazioni dell'Organizzazione. Svolgerà le seguenti funzioni:

- Istituzione dei requisiti dell'informazione in materia di sicurezza.
- Lavoro in collaborazione con il responsabile della sicurezza e il sistema per il mantenimento dei sistemi catalogati secondo l'Allegato I dello Schema Nazionale di valutazione della Sicurezza.

Responsabile dei servizi TIC

Il Dirigente avrà il ruolo di responsabile per i servizi TIC dell'organizzazione.Svolgerà le seguenti funzioni:

- Definizione dei requisiti dei servizi TIC in materia di sicurezza.
- Lavoro in collaborazione con il responsabile della sicurezza e del sistema per il mantenimento dei sistemi catalogati secondo l'Allegato I dello Schema Nazionale di valutazione della Sicurezza.

Responsabile della sicurezza

Il Direttore del Servizio di Tecnologie dell'Informazione e delle Comunicazioni avrà il ruolo di responsabile della sicurezza dell'Organizzazione. Svolgerà le seguenti funzioni:

- Mantenere la sicurezza delle informazioni trattate e dei servizi forniti dai sistemi centrali TIC, nelle proprie aree di responsabilità.
- Promuovere la formazione e la consapevolezza del Servizio di Tecnologia dell'Informazione e della Comunicazione nell'ambito della sua sfera di responsabilità.
- Verificare che le misure di sicurezza stabilite siano adeguate per la protezione delle informazioni gestite e dei servizi forniti.
- Analizzare, completare e approvare tutta la documentazione relativa alla sicurezza del sistema.
- Monitorare lo stato di sicurezza del sistema fornito dagli strumenti di gestione degli eventi di sicurezza e dai meccanismi di controllo implementati nel sistema.
- Supporto e supervisione delle indagini sugli incidenti di sicurezza dalla notifica alla risoluzione.
- Redigere report periodici di sicurezza per il proprietario del sistema, inclusi gli incidenti più rilevanti del periodo.
- Approvazione delle procedure di sicurezza preparate dal Responsabile del Sistema.
- Elaborazione delle norme di sicurezza dell'entità.

La figura di "Responsabile per la Sicurezza" descritta dall'ENS, non coincide con quella di responsabile per la sicurezza e conservazione degli archivi informatici della UAL.

Responsabili del Sistema IT

I Direttori di Servizio del Servizio delle Tecnologie dell'Informazione e della Comunicazione sono designati come Responsabili del Sistema dell'Organizzazione.Svolgono le funzioni qui elencate sulla base della loro area di pertinenza:

- Sviluppare, utilizzare e mantenere il Sistema per l'intero ciclo di vita, delle sue specificità; predisposizione e verifica del suo corretto funzionamento.
- Definire la topologia e la politica di gestione del Sistema stabilendo i criteri di utilizzo e i servizi disponibili in esso.
- Definire la politica di connessione o disconnessione di apparecchiature e nuovi utenti nel Sistema.
- Approvare le modifiche che influiscono sulla sicurezza della modalità operativa del sistema.
- Decidere le misure di sicurezza che saranno applicate dai somministratori delle componenti del Sistema durante le fasi di sviluppo, installazione e collaudo degli stessi.

- Impiantare e controllare le misure specifiche di sicurezza del Sistema e assicurarsi che siano correttamente integrate nel quadro generale di sicurezza.
- Determinare la configurazione autorizzata di hardware e software, da utilizzare nel sistema.
- Approvare qualsiasi modifica sostanziale della configurazione di qualsiasi elemento del Sistema.
- Eseguire il processo obbligatorio di analisi e gestione dei rischi nel sistema.
- Determinare la categoria del sistema secondo la procedura descritta nell'allegato I dell'ENS e determinare le misure di sicurezza da applicare come descritto nell'allegato II dell'ENS.
- Elaborare e approvare la documentazione di sicurezza del sistema.
- Delimitare le responsabilità di ciascuna entità coinvolta nel mantenimento, gestione, implementazione e supervisione del Sistema.
- *Garantire la conformità con gli obblighi del "Administrador de Seguridad del Sistema" (ASS).*
- Esame degli incidenti di sicurezza che interessano il sistema e comunicazione al responsabile della sicurezza o a chiunque esso determini.
- Stabilire piani di contingenza e di emergenza, includendo frequenti esercitazioni per l'addestramento del personale in relazione ad esse.
- Inoltre, il responsabile del sistema può predisporre la sospensione del trattamento di determinate informazioni o la fornitura di un determinato servizio qualora venga a a conoscenza di gravi carenze di sicurezza che potrebbero influire sulla soddisfazione dei requisiti stabiliti. Tale decisione deve essere concordata con i responsabili delle informazioni interessate, il servizio interessato e il responsabile della sicurezza, prima di essere eseguita.
- Preparazione delle necessarie procedure di sicurezza per l'operatività nel sistema.

Amministratore della Sicurezza del Sistema

L'Amministratore dei Servizi di Rete e Sicurezza TIC avrà il ruolo di Amministratore della Sicurezza del Sistema. Svolgerà le seguenti funzioni:

- Verificare l'approvazione delle procedure operative di sicurezza
- Garantire la conformità con i controlli di sicurezza
- Assicurarsi che vengano applicate le procedure approvate per la gestione del sistema informativo
- Supervisionare le installazioni hardware e software, le loro modifiche e miglioramenti per garantire che la sicurezza non sia compromessa e che siano sempre conformi alle autorizzazioni pertinenti
- Supervisionare il monitoraggio dello stato della sicurezza del sistema

- Informare i Responsabili della Sicurezza e del Sistema di qualunque anomalia, compromissione o vulnerabilità correlata alla sicurezza
- Collaborare nelle indagini e nella risoluzione degli incidenti di sicurezza, dal rilevamento alla risoluzione.

5.4 .POLITICA DI SICUREZZA

Sarà missione della Commissione di Sicurezza la revisione annuale di questa politica di Sicurezza delle Informazioni e la proposta di revisione o mantenimento della stessa.La Politica sarà approvata dal Consiglio di Governo e diffusa in modo che tutte le parti interessate ne siano a conoscenza.

6.DATI DI CARATTERE PERSONALE

La UAL realizza trattamenti in cui fa uso di dati personali, adottando le opportune misure di sicurezza seguendo le linee guida della Normativa Europea sulla Protezione dei Dati, le indicazioni del Delegato per la Protezione dei Dati in maniera tale da rispettare il principio di responsabilità proattiva e il principio di responsabilità stabiliti dall'attuale normativa per la sicurezza.

7.GESTIONE DEL RISCHIO

Tutti i sistemi soggetti a questa politica devono eseguire un'analisi dei rischi, valutando le minacce e i rischi a cui sono esposti. Questa analisi sarà ripetuta:

- Regolarmente, almeno una volta ogni due anni
- Quando le informazioni gestite cambiano
- Quando i servizi resi cambiano
- Quando si verifica un grave incidente di sicurezza
- Quando vengono segnalate gravi vulnerabilità
- Quando indicato dal Delegato per la protezione dei dati.

Per l'armonizzazione dell'analisi dei rischi, la Commissione per la Sicurezza stabilirà una valutazione di riferimento per i diversi tipi di informazioni gestite e i diversi servizi forniti.

Il Comitato per la Sicurezza delle TIC razionalizzerà la disponibilità di risorse per soddisfare le esigenze di sicurezza dei diversi sistemi, promuovendo investimenti orizzontali.

8.SVILUPPO DELLA POLITICA DI SICUREZZA

Questa politica sarà sviluppata attraverso regolamenti di sicurezza che affrontano aspetti specifici. Le norme di sicurezza saranno disponibili per tutti i membri dell'organizzazione che devono conoscerla, in particolare per coloro che utilizzano, gestiscono o amministrano i sistemi di informazione e comunicazione.

Le norme di sicurezza saranno disponibili sulla intranet, attraverso il portale di amministrazione elettronica (http://ae.ual.es) e il sito Web della Commissione per la Sicurezza (http://seguridad.ual.es)

Tale normativa potrà essere disponibile su supporto stampato presso il Servizio di Tecnologia dell'Informazione e delle Comunicazioni.

9.OBBLIGHI DEL PERSONALE

Tutti i membri della UAL hanno l'obbligo di conoscere e rispettare questa Politica di Sicurezza delle Informazioni e la Normativa di Sicurezza derivata da essa, essendo responsabilità della Commissione di Sicurezza di predisporre i mezzi necessari affinché l'informazione raggiunga i destinatari interessati.

Tutti i lavoratori UAL parteciperanno ad un'azione di sensibilizzazione alla sicurezza TICalmeno una volta ogni due anni .Sarà istituito un **programma di azioni per la sensibilizzazione** continua per il coinvolgimento di tutti i membri della UAL, in particolare dei nuovi membri, tenendo sempre conto della disponibilità di bilancio dell'Università.

Le persone responsabili dell'uso, della gestione o dell'amministrazione dei sistemi TIC riceveranno una formazione specifica per la gestione sicura dei sistemi, in base alle loro esigenze professionali. La formazione sarà obbligatoria e previa all'assunzione di responsabilità, sia che si tratti del primo incarico sia che si tratti di un cambiamento di tipologia di ruolo professionale o di responsabilità in esso.

10.TERZE PARTI

Nel caso in cui la UAL fornisca servizi ad altre organizzazioni o gestisca le informazioni di altre organizzazioni, esse saranno coinvolte in questa politica di sicurezza delle informazioni .A tal fine, saranno stabiliti canali per la segnalazione e il coordinamento dei rispettivi Comitati di Coordinamento dell'ENS e verranno stabilite le procedure per la reazione agli incidenti di sicurezza.

L'utilizzazione da parte della UAL di servizi di terze parti o il trasferimento di informazioni a terzi, presuporrà il coinvolgimento delle terze parti in questa Politica di Sicurezza e nella Politica di Sicurezza relativa a tali servizi o informazioni.Tale terza parte sarà soggetta agli obblighi stabiliti nei suddetti regolamenti e potrà sviluppare le proprie procedure operative in ottemperanza alla normativa vigente.Verranno stabilite procedure specifiche per la segnalazione e la risoluzione degli incidenti.Sarà garantito che il personale di terze

parti sia adeguatamente competente in materia di sicurezza, come stabilito nella presente Politica. Quando alcuni aspetti della Politica non possono essere soddisfatti da una terza parte , come richiesto nei paragrafi precedenti, sarà richiesto un rapporto dal Responsabile della Sicurezza per specificare i rischi che si presentano e il modo di affrontarli.
Il rapporto deve essere previamente a qualunque azione, approvato dai responsabili delle informazioni e dei servizi interessati.

11. ENTRATA IN VIGORE

Questa politica di Sicurezza delle Informazioni è efficace dal giorno successivo alla data di approvazione da parte del Consiglio Direttivo della UAL e fino a quando non venga sostituita da una nuova Politica.

Si intende abrogata la precedente Politica di Sicurezza delle Informazioni approvata dal Consiglio direttivo dell'Università di Almería, il 17 dicembre 2012.

1

---

[1] ERP = Sistema de Planificación de Recursos Empresariales.Dall'inglese *Enterprise Resource Planning*