



*Università Politecnica delle Marche*

## **DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

*(in ottemperanza a quanto previsto dal D.Lgs. 196 del 30 giugno 2003 e successive modifiche)*

**Versione 1.0**



## **ASPETTI GENERALI**

### **Campo di applicazione e obiettivi del documento.**

Il presente Documento Programmatico sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento di dati personali e/o sensibili effettuati con strumenti elettronici di elaborazione all'interno dell'Università Politecnica delle Marche. Il documento soddisfa tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti i soggetti dell'Università che trattano dati personali, conformemente a quanto previsto dal D.Lgs. 196 del 30 giugno 2003, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza. L'obiettivo del documento è quindi quello di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In particolare nel Documento Programmatico sulla Sicurezza sono definiti i criteri tecnici ed organizzativi per:

- a) La protezione delle aree e dei locali interessati dalle misure di sicurezza , nonché le procedure per controllare l'accesso alle persone autorizzate ai medesimi locali
- b) I criteri e le procedure per assicurare l'integrità dei dati
- c) L'elaborazione di un piano di formazione per rendere edotti gli incaricati al trattamento dei rischi individuati e dei modi per prevenire i danni

Il documento, facendo anche riferimento al Disciplinare Tecnico in Materia di Misure Minime di Sicurezza, Allegato B al D.Lgs n. 196 ed in particolare all'articolo 19 del suddetto allegato che descrive i contenuti del Documento Programmatico sulla sicurezza, si articola nelle seguenti sezioni:

1. Organizzazione dell'Università Politecnica delle Marche
2. Struttura della rete di Ateneo
3. Elenco dei trattamenti dei dati personali
4. Distribuzione dei compiti e delle responsabilità
5. Caratteristiche delle aree e dei locali, nonché degli strumenti con cui si effettuano i trattamenti
6. Analisi dei rischi che incombono sui dati
7. Misure in essere o da adottare per garantire l'integrità e la disponibilità dei dati



# *Università Politecnica delle Marche*

8. Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
9. Interventi formativi per gli incaricati
10. Criteri da adottare per l'adozione delle misure minime di sicurezza nei casi di trattamenti affidati all'esterno
11. Criteri da adottare in caso di dati sensibili e giudiziari

## **Organizzazione Università Politecnica delle Marche**

L'Università Politecnica delle Marche è organizzata in strutture primarie e derivate oltre alle Aziende e all'Amministrazione Centrale (Art. 21, 22, 23 e 24 dello Statuto). L'Amministrazione Centrale è organizzata in Servizi e Centri Tecnici (Ordinanza Dirigenziale n. 216 del 02.05.2005). Tale organizzazione individua quindi anche le strutture dell'Università Politecnica delle Marche interessate al trattamento di dati personali con strumenti informatici e riportate nell'elenco seguente:

### **Amministrazione**

Struttura amministrativa a supporto al Rettore  
Direzione Amministrativa + Il dirigente  
Servizio Programmazione e Controllo di Gestione  
Servizio Affari Generali e Ricerca  
Servizio Didattica  
Servizio Personale Tec. Amm.vo, Stipendi e Pensioni  
Servizio Economico Finanziario  
Servizio Innovazione e Trasferimento Tecnologico  
Servizio Provveditorato, Economato e Patrimonio  
Servizio Legale  
Servizio Amministrativo Polo Clinico (Didattica e Sanita')  
Centro Gestione e Sviluppo Edilizia  
Nucleo Informatico Amministrativo

### **Facoltà di AGRARIA**

Presidenza Facoltà di Agraria  
Azienda agraria  
Dipartimento di Scienze Ambientali e delle Produzioni Vegetali  
Dipartimento di Scienze Applicate ai Sistemi Complessi  
Dipartimento di Scienze degli Alimenti  
Istituto Biotecnologie Biochimiche

### **Facoltà di ECONOMIA "Giorgio Fuà"**

Presidenza Facoltà di Economia  
Dipartimento di Economia  
Dipartimento di Scienze Sociali  
Dipartimento Management e Organizzazione Industriale



## **Facolta' di INGEGNERIA**

Presidenza Facolta' di Ingegneria

Dipartimento Architettura, Rilievo, Disegno, Urbanistica, Storia

Dipartimento di Architettura, Costruzioni e Strutture

Dipartimento di Elettromagnetismo e Bioingegneria

Dipartimento di Elettronica, Intelligenza Artificiale e Telecomunicazioni

Dipartimento di Energetica

Dipartimento di Fisica e Ingegneria Materiali e Territorio

Dipartimento di Ingegneria Informatica, Gestionale e dell'Automazione

Dipartimento di Meccanica

Dipartimento di Scienze Matematiche

Dipartimento Scienze dei Materiali e della Terra

Istituto di Idraulica e Infrastrutture viarie

## **Facolta' di MEDICINA e CHIRURGIA**

Presidenza Facolta' di Medicina e Chirurgia

Dipartimento di Neuroscienze

Dipartimento di Patologia Molecolare e Terapie Innovative

Dipartimento di Scienze Mediche e Chirurgiche

Istituto Biotecnologie Biochimiche

Istituto di Biochimica

Istituto di Biologia e Genetica

Istituto di Malattie Infettive e Medicina Pubblica

Istituto di Medicina Clinica e Biotecnologie Applicate

Istituto di Microbiologia e Scienze Biomediche

Istituto di Morfologia Umana Normale

Istituto di Radiologia

Istituto di Scienze Materno-Infantili

Istituto di Scienze Odontostomatologiche

## **Facolta' di SCIENZE**

Dipartimento Scienze del Mare

Presidenza Facoltà di Scienze

## **Centri Interfacolta'**

Centro Ateneo di Documentazione

Centro di Supporto per l'Apprendimento delle Lingue

Centro Servizi Multimediali ed Informatici

In particolare l'Amministrazione Centrale effettua trattamenti sui dati personali relativi alla attività amministrativa istituzionale dell'Ateneo e inerente ai seguenti settori:

- gestione giuridica ed economica del personale
- gestione didattica e amministrativa degli studenti iscritti ai corsi di laurea dell'Ateneo
- gestione finanziaria, economica e patrimoniale
- gestione documentale e protocollo informatico



# *Università Politecnica delle Marche*

- gestione dati relativi a personale esterno in relazione all'espletamento di concorsi di varia natura
- gestione delle biblioteche di Ateneo

Le strutture decentrate (Facoltà, Istituti, Dipartimenti e Centri) effettuano trattamenti su dati personali in relazione alla attività di didattica e di ricerca di ogni singola struttura, dati che quindi in generale sono inerenti a:

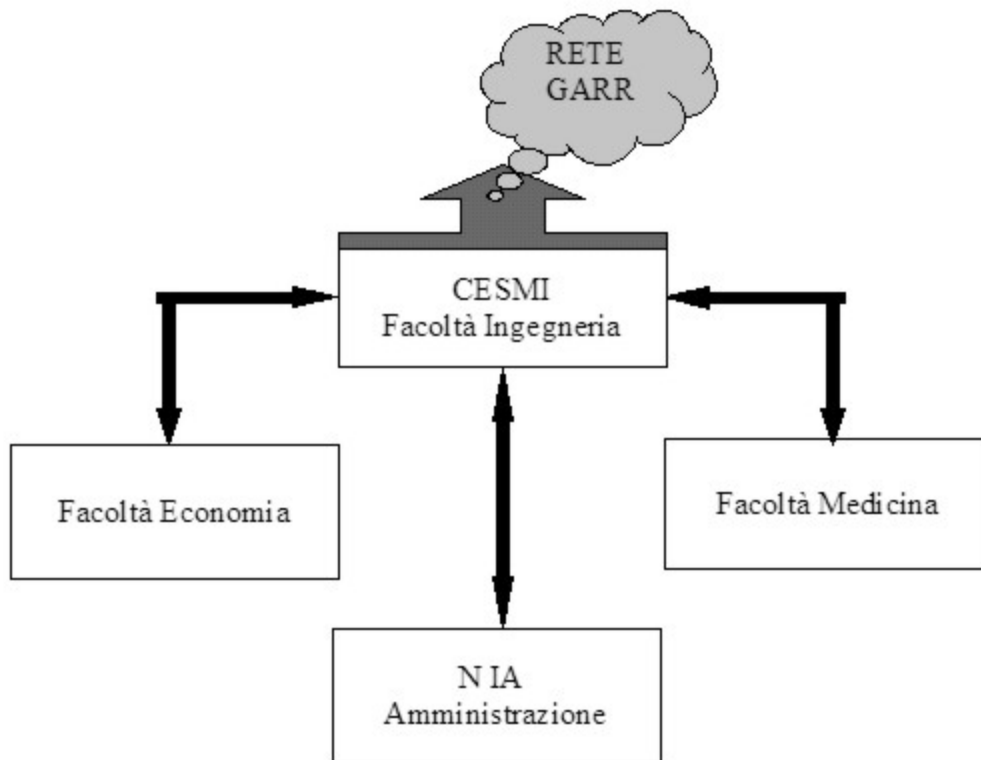
- personale strutturato e non che opera all'interno della struttura
- fornitori
- studenti che seguono corsi i cui titolari sono docenti afferenti alla struttura stessa
- dati relativi a ricerche scientifiche e test di laboratorio

L'organizzazione dell'Università Politecnica delle Marche si riflette anche sul presente Documento Programmatico sulla Sicurezza la cui struttura principale sarà relativa ai trattamenti inerenti alla attività della Amministrazione Centrale; al documento sono quindi allegati una serie di schede relative ai trattamenti inerenti alle varie strutture, a partire dalle Facoltà fino ai dipartimenti, agli istituti ed ai centri interfacoltà.

## **Architettura rete di Ateneo**

Tutti i trattamenti di dati personali sono effettuati utilizzando l'infrastruttura di rete dell'Ateneo la cui architettura è mostrata nella figura 1. La rete collega i quattro poli dell'Università Politecnica delle Marche con il centro stella situato presso il Polo di Monte Dago – Facoltà di Ingegneria all'interno del Centro Servizi Multimediali e Informatici. Al Polo di Monte Dago sono collegati con linee CDN a 2 Mb la Facoltà di Economia, la Facoltà di Medicina e l'Amministrazione Centrale attraverso il Nucleo Informatico Amministrativo. All'interno dei singoli Poli esistono altrettanti reti locali realizzate con cablaggio in fibra e/o in rame. Le due strutture portanti di questa architettura sono quindi il CESMI che gestisce la rete di Ateneo, la sicurezza della rete ed il collegamento con la rete GARR della ricerca, ed il NIA che gestisce tutte le procedure amministrative di Ateneo ed i relativi dati personali e sensibili sottoposti ai trattamenti relativi alla attività istituzionale.

## **Figura 1 – Architettura rete di Ateneo**



## ANALISI DEI TRATTAMENTI

### Premesse

In questa seconda parte del documento sono analizzati e descritti i vari trattamenti in essere presso l'Università Politecnica delle Marche, le responsabilità delle varie strutture per i diversi trattamenti, l'analisi dei rischi e le misure adottate per contrastarli come previsto dall'articolo 19 del Disciplinare Tecnico, Allegato B al D.Lgs. 196. Quanto descritto nelle sezioni successive in relazione alle varie regole, riguarda i trattamenti effettuati a livello centralizzato dalla Amministrazione Centrale, tutti i trattamenti a cura delle strutture periferiche sono descritti negli allegati A, B, C, D ed E relativi rispettivamente alle Facoltà di Agraria, Economia, Ingegneria, Medicina e Scienze che quindi costituiscono parte integrante del presente documento. La redazione e l'aggiornamento dei suddetti allegati sono a cura dei responsabili delle varie strutture periferiche che ne curano la trasmissione alla Amministrazione Centrale affinché possano diventare parte integrante del Documento Programmatico sulla Sicurezza dell'Università Politecnica delle Marche.



# *Università Politecnica delle Marche*

## **Elenco dei trattamenti dei dati personali (Regola 19.1)**

In questa sezione sono individuati tutti i trattamenti effettuati dall'Università Politecnica delle Marche, direttamente o attraverso collaborazioni esterne, facendo riferimento alla regola 19.1 dell'allegato tecnico al D.Lgs. 196. I trattamenti sono elencati nella tabella 1 dove sono riportate le seguenti informazioni:

Codice: codice identificativo di ogni singolo trattamento

Descrizione sintetica: indicazione della finalità perseguita o dell'attività svolta con il trattamento

Categoria persone: si individuano le categorie dei soggetti i cui dati personali sono sottoposti al relativo trattamento

Natura: indicazione della natura dei dati (p: personali, s:sensibili, g:giudiziari)

Struttura di riferimento: è indicata la struttura dell'Università Politecnica delle Marche all'interno della quale si effettua il trattamento in questione

Altre strutture: eventuali altre strutture anche esterne che concorrono al trattamento dei dati

Tipologia strumenti elettronici: sono individuati gli strumenti elettronici attraverso i quali si effettua il trattamento

## **Ulteriori elementi per descrivere i trattamenti di dati personali**

In questa sezione, che fa sempre riferimento alla regola 19.1 del disciplinare tecnico, sono illustrati ulteriori elementi descrittivi dei diversi trattamenti elencati nella tabella 1. Per ogni trattamento, identificato dal relativo codice, nella tabella 2 sono riportate le seguenti informazioni:

Banca dati: è individuata la banca dati o il data base o l'archivio informatico i cui i dati sono contenuti

Applicazione: è individuata l'applicazione relativa al trattamento di riferimento ed alla banca dati che l'applicazione stessa utilizza per effettuare il trattamento

Ubicazione fisica dei dati: si individua il luogo fisico dove i dati del trattamento e della relativa banca dati sono mantenuti, ovvero dove si trovano gli elaboratori sui cui dischi sono mantenuti i dati e i luoghi di conservazione dei supporti fisici dei dati siano essi i dati originali o le eventuali copie di sicurezza

Elaboratore: è individuato il tipo di elaboratore sul quale risiede la banca dati relativa al trattamento in questione



# *Università Politecnica delle Marche*

Conservazione supporti copie: si individuano i supporti attraverso i quali sono mantenute le copie di sicurezza della banca dati relativa al trattamento in questione

Dispositivi di accesso: in questa colonna sono elencati i dispositivi e gli strumenti attraverso i quali gli incaricati effettuano i trattamenti sulla banca dati in questione

Tipologia di interconnessione: individuazione del tipo di interconnessione che consente agli incaricati di effettuare i trattamenti e di accedere alla banca dati in questione

Note: per quanto riguarda i trattamenti AMM012, AMM013 e AMM014 si tratta di trattamenti a carico del Dipartimento della Funzione Pubblica e della Direzione Generale dell'INDAP per i quali non sono conosciuti né i tipi di elaboratore utilizzati né le modalità di conservazione delle eventuali copie dei dati. Gli incaricati dell'Università Politecnica delle Marche si limitano al caricamento dei dati utilizzando le procedure messe a disposizione dagli enti sopra citati.



**Tabella 1 – Regola 19.1 dell’Allegato B – ELENCO DEI TRATTAMENTI PERSONALI – Informazioni essenziali**

Codice	Descrizione sintetica	Categorie persone	Natura	Struttura di riferimento	Altre strutture	Tipologia strumenti elettronici
AMM000	Gestione utenti per accesso al dominio ed alla rete della Amministrazione Centrale	Personale Docente e Tecnico Amministrativo	P	Nucleo Informatico Amministrativo (NIA)	CESMI	Server Windows
AMM001	Gestione utenti portale di Ateneo	Personale Docente e Tecnico Amministrativo, Studenti	P	Nucleo Informatico Amministrativo CESMI		Server Windows
AMM100	Carriera giuridica ed economica del personale ai fini del calcolo del trattamento economico	Personale Docente e Tecnico Amministrativo	S	Direzione Amministrativa - Servizio Personale Tecnico Amministrativo - Servizio Medicina e Sanità	NIA, Cineca	Elaboratore centrale e personal computer collegati in rete locale in modalità client/server
AMM101	Orari di servizio del personale ai fini del controllo della presenza in servizio e della gestione delle assenze di varia natura	Personale Tecnico Amministrativo	P	Servizio Personale Tecnico Amministrativo	NIA	Elaboratore centrale e personal computer collegati in rete locale con procedure web-oriented
AMM102	Anagrafe delle prestazioni	Personale Docente e Tecnico Amministrativo	P	Direzione Amministrativa - Servizio Personale Tecnico Amministrativo - Centro Sviluppo e Gestione Edilizia	Dipartimento Funzione Pubblica	Personal computer collegati ad Internet con procedure Web
AMM103	Gestione distacchi, permessi, aspettative sindacali	Personale Docente e Tecnico Amministrativo	S	Direzione Amministrativa - Servizio Personale Tecnico Amministrativo	Dipartimento Funzione Pubblica	Personal computer collegati ad Internet con procedure Web
AMM104	Trattamento pensionistico	Personale Docente e Tecnico Amministrativo	P	Direzione Amministrativa - Servizio Personale Tecnico Amministrativo	INPDAP Direzione generale	Personal computer



**Tabella 1 – Regola 19.1 dell’Allegato B – ELENCO DEI TRATTAMENTI PERSONALI – Informazioni essenziali**

<b>Codice</b>	<b>Descrizione sintetica</b>	<b>Categorie persone</b>	<b>Natura</b>	<b>Struttura di riferimento</b>	<b>Altre strutture</b>	<b>Tipologia strumenti elettronici</b>
AMM105	Affidamento incarichi di docenza, coordinamento, tutorato e guida al personale del S.S.N	Personale del S.S.N.	P	Servizio Sanità		Personal computer
AMM106	Controllo fisico sanitario per rischi non convenzionali	Personale Docente e Tecnico Amministrativo	S	Centro Sviluppo e Gestione Edilizia	Servizio Personale, Azienda Sanitaria	Personal computer
AMM107	Gestione visite per assunzioni ed idoneità	Personale Docente e Tecnico Amministrativo	S	Centro Sviluppo e Gestione Edilizia	Servizio personale, Medicina del Lavoro	Personal computer
AMM108	Gestione autorizzazioni per parcheggi università	Personale Docente e Tecnico Amministrativo	P	Servizio Provveditorato, Economato e Patrimonio		Personal computer
AMM109	Gestione elezioni rappresentanti organi accademici	Personale Docente e Tecnico Amministrativo	P	Servizio Affari Generali e Ricerca	Servizio Personale	Personal Computer
AMM200	Gestione carriere didattiche ai fini del conseguimento del titolo di studio	Studenti	S	Servizio Didattica - Servizio Medicina e Sanità	NIA, Cineca	Elaboratore centrale e personal computers collegati in rete locale e geografica in modalità client/server
AMM201	Determinazione tassa personalizzata	Studenti	P	Servizio Didattica	NIA	Server centrale e personal computer



**Tabella 1 – Regola 19.1 dell’Allegato B – ELENCO DEI TRATTAMENTI PERSONALI – Informazioni essenziali**

Codice	Descrizione sintetica	Categorie persone	Natura	Struttura di riferimento	Altre strutture	Tipologia strumenti elettronici
AMM202	Gestione tasse per pagamento contributi	Studenti	P	Servizio Didattica	NIA, Unicredito	Server centrale e personal computer
AMM203	Fornitura beni e servizi per studenti disabili	Studenti	S	Servizio Didattica	NIA, Ersu	Personal computer
AMM204	Consultazione dati carriera	Studenti	P	Servizio Didattica	NIA	Server centrale con procedure Web
AMM205	Gestione autorizzazioni per parcheggi università	Studenti	P	Servizio Provveditorato, Economato e Patrimonio		Personal computer
AMM206	Gestione elezioni rappresentanti organi accademici e studenteschi	Studenti	P	Servizio Affari Generali e Ricerca	Servizio Didattica	Personal computer
AMM300	Attività relative al trattamento di dati economico, patrimoniali e finanziari inerenti la gestione del bilancio	Fornitori esterni, Personale Docente e Tecnico Amministrativo, Studenti	P	Servizio Contabilità Generale - Servizio Economato e patrimonio	NIA, Tutte le strutture amministrative centrali e periferiche	Elaboratore centrale e personal computers collegati in rete locale e geografica in modalità client/server
AMM400	Attività inerenti la gestione del protocollo e dei documenti elettronici	Persone fisiche e giuridiche esterne, Personale Docente e Tecnico Amministrativo, Studenti	P	Direzione Amministrativa	NIA, Servizi, Strutture amministrative periferiche	Elaboratore centrale e personal computer collegati in rete locale con procedure web-oriented



**Tabella 1 – Regola 19.1 dell’Allegato B – ELENCO DEI TRATTAMENTI PERSONALI – Informazioni essenziali**

Codice	Descrizione sintetica	Categorie persone	Natura	Struttura di riferimento	Altre strutture	Tipologia strumenti elettronici
AMM401	Attività amministrativa ordinaria e straordinaria	Persone fisiche e giuridiche esterne, Personale Docente e Tecnico Amministrativo, Studenti	S	Direzione Amministrativa Servizi	NIA	File servers e personal computers
AMM402	Gestione archivio documenti gare	Persone fisiche e giuridiche esterne	S	Servizio Legale	Servizi Amministrazione	Personal computers
AMM500	Sito web di Ateneo e servizi collegati	Persone fisiche e giuridiche esterne, Personale Docente e Tecnico Amministrativo, Studenti	P	Nucleo Informatico Amministrativo (NIA)	Servizi amministrazione centrale	Server Windows
AMM600	Gestione archivio bibliografico delle Facoltà per consultazione e prestito	Personale Docente e Tecnico Amministrativo Studenti	P	Centro Ateneo di Documentazione	NIA	Elaboratore centrale e personal computer collegati in rete geografica in modalita' client/server



**Tabella 2 - Regola 19.1 dell'Allegato B - ELENCO TRATTAMENTI DATI PERSONALI - Ulteriori elementi descrittivi degli strumenti utilizzati**

<b>Codice</b>	<b>Banca Dati</b>	<b>Applicazione</b>	<b>Ubicazione fisica dati</b>	<b>Elaboratore</b>	<b>Conservazione supporti copie</b>	<b>Dispositivi di accesso</b>	<b>Tipologia interconnessioni</b>
AMM000	Utenti Windows	Windows 2000 Server, PLSQL	Nucleo Informatico Amministrativo	Server Windows	Nastro magnetico sistema backup	Personal Computer Windows	Rete Locale e Geografica
AMM001	Utenti Portale	Windows 2000 Sever	Nucleo Informatico Amministrativo	Server Windows con Data Base Oracle	Nastro magnetico sistema backup	Browser	Internet
AMM100	DB CSA Oracle	CSA	Nucleo Informatico Amministrativo	RISC IBM	Nastro magnetico sistema backup	Personal Computer Windows	Rete Locale
AMM101	DB Orari Oracle	OrariWeb	Nucleo Informatico Amministrativo	RISC IBM	Nastro magnetico sistema backup	Personal Computer Windows	Rete Locale e Internet per la consultazione
AMM102	Prestazioni	Procedura web x inserimento dati	Dipartimento della Funzione Pubblica			Personal Computer Windows	Rete Internet
AMM103	Banca Dati Funzione Pubblica	Procedura web x inserimento dati	Dipartimento della Funzione Pubblica			Personal Computer Windows	Rete Internet



**Tabella 2 - Regola 19.1 dell'Allegato B - ELENCO TRATTAMENTI DATI PERSONALI - Ulteriori elementi descrittivi degli strumenti utilizzati**

<b>Codice</b>	<b>Banca Dati</b>	<b>Applicazione</b>	<b>Ubicazione fisica dati</b>	<b>Elaboratore</b>	<b>Conservazione supporti copie</b>	<b>Dispositivi di accesso</b>	<b>Tipologia interconnessioni</b>
AMM104	Banca Dati INPDAP	Procedura web x inserimento dati	INPDAP - Direzione Generale			Personal Computer Windows	Rete Internet
AMM105	Files su personal computer	Word, Excel	Servizio Sanità Facoltà Medicina	Personal computer	Nastro magnetico sistema backuo	Personal Computer Windows	Rete locale
AMM106	Files su personal computer	Office automation	Centro Gestione e Sviluppo Edilizia	Personal computer	Nastro magnetico sistema backuo	Personal computer Windows	Rete locale
AMM107	Files su personal computer	Office automation	Centro Gestione e Sviluppo Edilizia	Personal computer	Nastro magnetico sistema backuo	Personal computer Windows	Rete locale
AMM108	Files su personal computer	Office automation	Servizio Provveditorato, Economato e Patrimonio	Pc Windows	Nastro magnetico sistema backuo	Personal computer windows	Rete Locale
AMM109	Files su personal computer	Office automation	Servizio Affari Generali e Ricerca	Pc Windows	Nastro magnetico sistema backup	Personal computer windows	Rete locale



**Tabella 2 - Regola 19.1 dell'Allegato B - ELENCO TRATTAMENTI DATI PERSONALI - Ulteriori elementi descrittivi degli strumenti utilizzati**

Codice	Banca Dati	Applicazione	Ubicazione fisica dati	Elaboratore	Conservazione supporti copie	Dispositivi di accesso	Tipologia interconnessioni
AMM200	DB GISS Oracle	GISS	Nucleo Informatico Amministrativo	RISC IBM	Nastro magnetico sistema backup	Personal Computer Windows Terminale intelligente	Rete Locale, Rete Geografica, Internet
AMM201	Archivio autocertificazioni, archivio carriere	GISS, Procedura tassa personalizzata	Nucleo Informatico Amministrativo	RISC IBM, Server Windows	Nastro magnetico sistema backup	Personal Computer Windows	Rete Locale, Internet
AMM202	Archivio carriere	GISS	Nucleo Informatico Amministrativo	RISC IBM, Server Windows	Nastro magnetico sistema backup	Personal computer windows	Rete locale, internet
AMM203	Archivio dati locale	Office automation	Servizio Didattica, Nucleo Informatico Amministrativo	RISC IBM, Server Windows	Nastro magnetico sistema backup	Personal computer windows	Rete locale, Internet
AMM204	DB carriera studenti	Procedure Java di consultazione	Nucleo Informatico Amministrativo	Windows 2000 Server	Nastro magnetico sistema di backup	Browser	Internet
AMM205	Files su personal computer	Office automation	Servizio Provveditorato, Economato e Patrimonio	Pc Windows	Nastro magnetico sistema backup	Personal computer windows	Rete locale



**Tabella 2 - Regola 19.1 dell'Allegato B - ELENCO TRATTAMENTI DATI PERSONALI - Ulteriori elementi descrittivi degli strumenti utilizzati**

<b>Codice</b>	<b>Banca Dati</b>	<b>Applicazione</b>	<b>Ubicazione fisica dati</b>	<b>Elaboratore</b>	<b>Conservazione supporti copie</b>	<b>Dispositivi di accesso</b>	<b>Tipologia interconnessioni</b>
AMM206	Files su personal computer	Office automation	Servizio Affari Generali e Ricerca	Pc Windows	Nastro magnetico sistema backup	Personal computer windows	Rete locale
AMM300	DB CIA Oracle	CIA	Nucleo Informatico Amministrativo	RISC IBM	Nastro magnetico sistema backup	Personal Computer Windows Terminale intelligente	Rete Locale, Rete Geografica, Internet
AMM400	Protocollo Extraway	Titulus 97	Nucleo Informatico Amministrativo	RISC IBM	Nastro magnetico e CD in armadio ignifugo	Browser	Rete Locale
AMM401	File server	Office automation	Nucleo Informatico Amministrativo	Server Windows	Nastro magnetico sistema backup	Personal Computer Windows	Rete Locale e Geografica
AMM402	Archivio DB Extraway	Procedura personalizzata	Servizio Legale	Pc Windows	Memoria di massa esterna	Personal Computer Windows	Rete locale
AMM500	Data Base Oracle	Janus, Procedure di immissione dati via web	Nucleo Informatico Amministrativo	Server Windows	Nastro magnetico sistema backup	Personal Computer Windows	Internet



**Tabella 2 - Regola 19.1 dell'Allegato B - ELENCO TRATTAMENTI DATI PERSONALI - Ulteriori elementi descrittivi degli strumenti utilizzati**

<b>Codice</b>	<b>Banca Dati</b>	<b>Applicazione</b>	<b>Ubicazione fisica dati</b>	<b>Elaboratore</b>	<b>Conservazione supporti copie</b>	<b>Dispositivi di accesso</b>	<b>Tipologia interconnessioni</b>
AMM600	Anagrafica Utenti	Sebina	Nucleo Informativo Amministrativo	RISC IBM	Nastro magnetico sistema backup	Personal Computer Windows	Rete Locale e Geografica



## **Distribuzione dei compiti e delle responsabilità (Regola 19.2)**

In questa sezione si descrivono i compiti delle varie strutture dell'Ateneo e le relative responsabilità in relazione ai diversi trattamenti. Le informazioni sono raccolte nella tabella 3 dove sono riportati i seguenti dati:

Struttura: facendo riferimento alla organizzazione riportata precedentemente sono indicate le strutture addette ai vari trattamenti

Tipo trattamento: codice del trattamento come riportato nella tabella 1

Compiti e responsabilità della struttura: descrizione sintetica dei compiti e delle responsabilità rispetto ai trattamenti di competenza

Fra le varie strutture dell'Amministrazione Centrale, il Nucleo Informatico Amministrativo è la struttura che ha in gestione i vari server sui quali sono installate le base dati relative a tutti i dati personali oggetto dei diversi trattamenti. Il personale del Nucleo, avendo il compito di coadiuvare il personale amministrativo nell'utilizzo delle diverse procedure e dovendo gestire i server dal punto di vista sistemistico e del mantenimento dei dati, entra in gioco in tutti i trattamenti di dati personali effettuati a livello centrale.



**Tabella 3 - Regola 19.2 dell'Allegato B - DESCRIZIONI COMPITI E RESPONSABILITA' - Informazioni essenziali**

<b>Struttura</b>	<b>Tipo Trattamento</b>	<b>Compiti e responsabilita'</b>
<b>Struttura amministrativa</b>	AMM400	Inserimento dati protocollo in partenza
<b>supporto rettore</b>	AMM401	Predisposizione provvedimenti e delibere
<b>Direzione</b>	AMM100	Inserimento dati carriera giuridica ed economica personale docente
<b>Amministrativa</b>	AMM102	Inserimento dati
	AMM103	Inserimento dati
	AMM104	Inserimento dati
	AMM400	Inserimento dati posta in entrata ed in uscita
	AMM401	Predisposizione delibere degli organi accademici e provvedimenti vari
<b>Servizio Programmazione</b>	AMM300	Inserimento dati bilancio e attività economico-patrimoniale
<b>Controllo di Gestione</b>	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione provvedimenti e delibere
<b>Servizio Affari Generali e</b>	AMM109	Predisposizione liste elettorali ed elenchi e relative comunicazione



**Tabella 3 - Regola 19.2 dell'Allegato B - DESCRIZIONI COMPITI E RESPONSABILITA' - Informazioni essenziali**

<b>Struttura</b>	<b>Tipo Trattamento</b>	<b>Compiti e responsabilita'</b>
<b>Ricerca</b>	AMM206	Predisposizione liste elettorali ed elenchi e relative comunicazione
	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione provvedimenti e delibere
<b>Servizio Didattica</b>	AMM200	Inserimento dati, aggiornamento archivi carriere studenti, produzione statistiche
	AMM201	Inserimento dati relativi all'autocertificazione e regole di elaborazione
	AMM202	Controllo ed inserimento dati
	AMM203	Inserimento dati
	AMM400	Inserimento dati protocollo in uscita
	AMM401	Predisposizione delibere degli organi accademici
<b>Servizio Personale Tecnico</b>	AMM100	Inserimento dati carriera giuridica ed economica, calcolo e stampe
<b>Amministrativo, Stipendi e Pensioni</b>	AMM101	Inserimento dati, calcolo riepiloghi orari, stampe riepiloghi mensili
	AMM102	Inserimento dati



**Tabella 3 - Regola 19.2 dell'Allegato B - DESCRIZIONI COMPITI E RESPONSABILITA' - Informazioni essenziali**

<b>Struttura</b>	<b>Tipo Trattamento</b>	<b>Compiti e responsabilita'</b>
	AMM103	Inserimento dati
	AMM104	Inserimento dati
	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere degli organi accademici
<b>Servizio Economico</b>	AMM300	Inserimento dati relativi alla contabilità economico patrimoniale
<b>Finanziario</b>	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere e provvedimenti
<b>Servizio Innovazione e Trasferimento Tecnologico</b>	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere e provvedimenti
<b>Servizio Provveditorato, Economato e Patrimonio</b>	AMM108	Gestione autorizzazioni per accesso parcheggi
	AMM205	Gestione autorizzazioni per accesso parcheggi
	AMM300	Inserimento dati per gestione economico, finanziaria e patrimoniale



**Tabella 3 - Regola 19.2 dell'Allegato B - DESCRIZIONI COMPITI E RESPONSABILITA' - Informazioni essenziali**

<b>Struttura</b>	<b>Tipo Trattamento</b>	<b>Compiti e responsabilita'</b>
	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere e provvedimenti
<b>Servizio Legale</b>	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere e provvedimenti
	AMM402	Acquisizione documenti e inserimento dati
<b>Servizio Amministrativo</b>	AMM100	Inserimento dati carriera giuridica ed economica personale convenzionato, calcolo e stampe
<b>Polo Clinico</b>	AMM105	Inserimento dati e predisposizione provvedimenti
	AMM200	Inserimento dati carriere studenti facoltà di Medicina
	AMM300	Inserimento dati, emissione buoni ordine e mandati
	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere degli organi accademici
<b>Centro Gestione e</b>	AMM106	Inserimento, gestione, elaborazione dati anche ai fini della organizzazione delle visite



**Tabella 3 - Regola 19.2 dell'Allegato B - DESCRIZIONI COMPITI E RESPONSABILITA' - Informazioni essenziali**

<b>Struttura</b>	<b>Tipo Trattamento</b>	<b>Compiti e responsabilita'</b>
<b>Sviluppo Edilizia</b>	AMM107	Inserimento, gestione ed elaborazione dei dati
	AMM300	Inserimento dati relativi alle procedure di spesa: ordini, impegni, mandati, inventario
	AMM400	Inserimento dati protocollo in partenza
	AMM401	Predisposizione delibere degli organi accademici
<b>Nucleo</b>	AMM000	Gestione utenti, assegnazione delle password e gestione dei diritti di accesso alle risorse di rete
<b>Informatico</b>	AMM001	Procedure per la popolazione automatica del data base utenti portale dalle procedure CSA e GISS, gestione e manutenzione data base utenti
<b>Amministrativo</b>	AMM100	Gestione utenti, produzione statistiche, manutenzione archivi, procedure di integrazione con la contabilità, procedure di backup e di ripristino
	AMM101	Gestione utenti, manutenzione programmi, produzione statistiche, gestione tecnica operativa degli archivi, procedure di backup e di ripristino
	AMM200	Gestione utenti, manutenzione programmi, procedure di integrazione con la contabilita', gestione tecnica operativa degli archivi, procedure di backup e di ripristino
	AMM201	Manutenzione procedure, gestione tecnica e operativa degli archivi, procedure di backup e di ripristino
	AMM202	Manutenzione procedure, elaborazione, produzione e trasmissione all'ente tesoriere dei dati relativi alle tasse
	AMM204	Manutenzione procedure per la consultazione della carriera



**Tabella 3 - Regola 19.2 dell'Allegato B - DESCRIZIONI COMPITI E RESPONSABILITA' - Informazioni essenziali**

<b>Struttura</b>	<b>Tipo Trattamento</b>	<b>Compiti e responsabilita'</b>
	AMM300	Gestione utenti, produzione statistiche, manutenzione archivi, procedure di backup e di ripristino, inserimento dati relativi alle procedure di spesa: ordini, impegni, mandati, inventario
	AMM400	Gestione utenti, produzione statistiche, manutenzione archivi, procedure di backup e di ripristino, inserimento dati protocollo in partenza
	AMM401	Gestione diritti di accesso, gestione tecnica e operativa degli archivi, procedure di backup e di ripristino, Predisposizione delibere degli organi accademici
	AMM500	Manutenzione delle procedura via web, produzione dei documenti, Gestione tecnica e operativa degli archivi
	AMM600	Gestione utenti, produzione statistiche, manutenzione archivi, procedure di backup e di ripristino



## Analisi dei rischi che incombono sui dati (Regola 19.3)

In questa sezione è riportata un'analisi degli eventi potenzialmente dannosi per la sicurezza dei dati con le possibili conseguenze in termini di gravità. Gli eventi, descritti nella successiva tabella 4, sono stati suddivisi in tre categorie che riguardano il comportamento degli operatori (tabella 4.1), la strumentazione (tabella 4.2) ed il contesto fisico ambientale (tabella 4.3). Per ogni evento è fornita una breve valutazione delle conseguenze per la sicurezza dei dati in relazione sia alla rilevanza che alla probabilità stimata dell'evento.

**Tabella 4.1 - Regola 19.3 dell'Allegato B - ANALISI DEI RISCHI - Informazioni essenziali - Comportamento operatori**

Comportamento degli operatori		
<i>Rischio</i>	<i>Si/No</i>	<i>Descrizione impatto</i>
Sottrazione credenziali operatore	Si	Gravità medio/bassa che può comportare rischi relativi all'accesso ad informazioni riservate e rischi più contenuti in relazione all'aggiornamento degli archivi con dati non autorizzati in quanto tali eventualità comportano la conoscenza approfondita delle procedure che consentono la gestione dei dati
Carenza consapevolezza, disattenzione incuria	Si	Rischio basso sulla base della esperienza relativa al comportamento degli operatori delle varie procedure. L'evento potrebbe causare aggiornamenti non corretti degli archivi con conseguenze gravi soprattutto sui trattamenti AMM010, AMM020 e AMM030
Comportamenti sleali e fraudolenti	No	Sulla base della esperienze passate un simile rischio risulta essere altamente improbabile
Errore materiale	No	Errori che sfuggano al controllo delle procedure sono altamente improbabili e a basso rischio, stimato anche sulla esperienza passata

**Tabella 4.2 - Regola 19.3 dell'Allegato B - ANALISI DEI RISCHI - Informazioni essenziali - Eventi relativi agli strumenti**

Eventi relativi agli strumenti		
<i>Rischio</i>	<i>Si/No</i>	<i>Descrizione impatto</i>
Azione di virus o di programmi suscettibili di arrecare danno	Si	Rischio medio/basso in quanto tutti i computers sono dotati di programmi antivirus aggiornati. I rischi sono limitati agli archivi gestiti su computer con sistemi operativi Windows e posso portare alla perdita dei dati
Spamming o tecniche di sabotaggio	Si	Lo spamming ha effetti esclusivamente sulla posta elettronica e può avere conseguenze sulla eliminazione considerata erroneamente come spamming.



**Tabella 4.2 - Regola 19.3 dell'Allegato B - ANALISI DEI RISCHI - Informazioni essenziali - Eventi relativi agli strumenti**

<b>Eventi relativi agli strumenti</b>		
<b>Rischio</b>	<b>Si/No</b>	<b>Descrizione impatto</b>
Malfunzionamenti, indisponibilità o degrado degli strumenti	Si	Rischio basso per tutti i server centrali e medio per i dati conservati sui personal computer la cui conseguenza può arrivare alla perdita stessa dei dati
Accessi esterni non autorizzati	Si	Rischio basso per tutti i computer all'interno della rete della amministrazione protetta da firewall, medio per i computer all'interno delle facoltà. I rischi sono sempre circoscritti ai dati residenti su personal computers, più facilmente accessibili
Intercettazioni di informazioni in rete	Si	Rischio basso e circoscritto alla possibile visualizzazione di dati personali. Gli archivi di produzione non sono accessibili all'esterno della rete di ateneo

**Tabella 4.3 - Regola 19.3 dell'Allegato B - ANALISI DEI RISCHI - Informazioni essenziali - Eventi relativi all'ambiente**

<b>Eventi relativi al contesto fisico-ambientale</b>		
<b>Rischio</b>	<b>Si/No</b>	<b>Descrizione impatto</b>
Ingressi non autorizzati a locali	Si	Rischio medio in quanto i locali non sono adeguatamente protetti ma l'accesso ai computer è regolato da credenziali di accesso. Il rischio potrebbe causare la perdita di dati in conseguenza di atti vandalici
Sottrazione di strumenti contenenti dati	Si	Rischio medio legato alla mancata protezione dei locali, che potrebbe causare la perdita dei dati
Eventi distruttivi naturali o artificiali	Si	Rischio medio/basso la cui conseguenza potrebbe essere la perdita dei dati
Guasti a sistemi complementari	Si	Guasti relativi soprattutto alla alimentazione elettrica e all'impianto di condizionamento. Tali rischi potrebbero causare la perdita di dati
Errori umani nella gestione della sicurezza fisica	Si	Rischio della stessa entità degli altri rischi ambientali in quanto non esistono adeguati sistema di sicurezza ambientali. La causa principale potrebbe essere la perdita dei dati



## **Misure in essere e da adottare (Regola 19.4)**

In questa sezione, le cui informazioni sono raccolte nella successiva tabella 5, sono riportate tutte misure adottate o da adottare per contrastare i rischi sulla sicurezza dei dati analizzati ed elencati nella sezione precedente. Le informazioni riportate nella tabella sono le seguenti:

Misura: descrizione sintetica della misura adottata o da adottare

Descrizione del rischio: descrizione sintetica del rischio che si intende contrastare con la misura in questione

Trattamenti interessati: facendo riferimento alla tabella 1 sono riportati i codici dei trattamenti interessati dalla misura in questione

In essere/da adottare: si indica se la misura è già stata adottata oppure è in corso di attuazione ed eventualmente il termine temporale entro cui sarà messa in opera

Struttura addetta: si indica la struttura addetta all'adozione della misura stessa

L'allegato F al presente documento contiene una scheda descrittiva per ogni misura adottata e riportata nella tabella 5. Ogni scheda, a formato libero, contiene i seguenti elementi essenziali per descrivere la singola misura di sicurezza:

- il rischio che si intende contrastare
- la tipologia della misura (preventiva, di contrasto, di contenimento degli effetti)
- responsabilità dell'attuazione e della gestione della misura
- gli ambiti di applicazione (fisici, logici o procedurali)



**Tabella 5 - Regola 19.4 dell'Allegato B - MISURE SICUREZZA ADOTTATE O DA ADOTTARE**

<b>Codice</b>	<b>Misure</b>	<b>Rischi contrastati</b>	<b>Trattamenti interessati</b>	<b>In essere/Da adottare</b>	<b>Struttura o persone addette</b>
MIS001	Gestione password BIOS	Accessi non autorizzati	Tutti i trattamenti	In corso di adozione	Tutti i singoli utenti di ogni personal computer
MIS002	Gestione delle password di accesso al dominio Windows	Accessi non autorizzati Sottrazione delle credenziali	Tutti i trattamenti	In corso di adozione	Nucleo Informatico Amministrativo
MIS003	Politica di gestione delle password di accesso ai trattamenti	Accessi non autorizzati, Sottrazione credenziali	AMM100, AMM101, AMM200, AMM300, AMM400, AMM500, AMM600	Adottata	Nucleo Informatico Amministrativo
MIS004	Informazione sulle norme da seguire per l'utilizzo delle stazioni di lavoro	Carenza consapevolezza e disattenzione nell'utilizzo, Errori materiali	Tutti i trattamenti	Adottata	Tutti i responsabili dei trattamenti
MIS005	Aggiornamenti periodici degli utenti in merito all'utilizzo delle procedure	Sottrazione di credenziali, Errori materiali	Tutti i trattamenti	Adottata	Tutti i responsabili dei trattamenti
MIS006	Aggiornamento automatico e giornaliero dei programmi antivirus	Azione di virus informatici o programmi in grado di arrecare danno	Tutti i trattamenti	Adottata	Nucleo Informatico Amministrativo, CESMI
MIS007	Aggiornamento periodico delle attrezzature informatiche	Malfunzionamenti, indisponibilità o degrado degli strumenti	Tutti i trattamenti	Adottata	Nucleo Informatico Amministrativo e tutte le singole strutture periferiche



**Tabella 5 - Regola 19.4 dell'Allegato B - MISURE SICUREZZA ADOTTATE O DA ADOTTARE**

<b>Codice</b>	<b>Misure</b>	<b>Rischi contrastati</b>	<b>Trattamenti interessati</b>	<b>In essere/Da adottare</b>	<b>Struttura o persone addette</b>
MIS008	Firewall per il controllo della rete di Ateneo	Spamming, Tecniche di sabotaggio, Accessi non autorizzati, Intercettazione	Tutti i trattamenti	Adottata	Nucleo Informatico Amministrativo, CESMI
MIS009	Controllo degli accessi mediante utilizzo di smart card personali	Ingressi non autorizzati ai locali	Tutti i trattamenti	Da adottare nei prossimi 6 mesi	Amministrazione
MIS010	Conservazione copie in armadi ignifughi	Eventi distruttivi	AMM010, AMM011, AMM020, AMM030, AMM040, AMM050, AMM060	Adottata	Nucleo Informatico Amministrativo
MIS011	Procedura per crittografia dati sensibili	Diffusione dati sensibili a personale non autorizzato	AMM016, AMM017, AMM041	Adottata	Tutte le strutture che gestiscono dati sensibili, Nucleo Informatico Amministrativo



## **Criteri e modalità di ripristino della disponibilità dei dati (Regola 19.5)**

In questa sezione sono descritte le modalità e le procedure adottate per il ripristino dei dati in caso di loro danneggiamento o inaffidabilità dei data-base. Le informazioni relative a queste procedure sono illustrate nella tabella 6 in cui sono riportate le seguenti informazioni:

Banca dati: Archivio, data base o banca dati interessata alla procedura di ripristino

Criteri e procedure di salvataggio: descrizione sintetica delle modalità seguite nelle procedure di salvataggio dei dati

Luogo di custodia delle copie: luogo fisico dove sono mantenute le copie dei dati

Pianificazione delle prove di ripristino: tempi e modalità seguite nell'effettuare le prove di ripristino delle varie banche dati

Struttura incaricata del salvataggio: struttura dell'Ateneo incaricata del salvataggio e delle custodia dei dati



**Tabella 6 - Regola 19.5 dell'Allegato B - CRITERI E PROCEDURE PER IL SALVATAGGIO DEI DATI**

<b>Banca Dati</b>	<b>Criteri e procedure per salvataggio</b>	<b>Luogo custodia delle copie</b>	<b>Pianificazione prove ripristino</b>	<b>Struttura incaricata del salvataggio</b>
Utenti Windows	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Personale	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Orari	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Files su personal computer				
Archivio carriere	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Gestione economico patrimoniale	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Protocollo	Salvataggio giornaliero, copia settimanale su CD	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
File server	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Data Base Oracle	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete
Anagrafica Utenti	Salvataggio giornaliero	Nucleo Informatico Amministrativo	Prove di ripristino ogni 6 mesi	Nucleo Informatico Amministrativo - Ripartizione Gestione Sistemi e Servizi di Rete



## Pianificazione degli interventi formativi previsti (Regola 19.6)

Si prevedono una serie di interventi formativi, sia per i responsabili che per gli incaricati al trattamento dei dati personali attraverso le diverse procedure indicate nelle tabelle 1 e 2, che si diversificano a seconda del momento in cui gli interventi stessi sono effettuati. I momenti sono determinati dagli eventi con indicato il tipo di intervento formativo come indicato nella tabella seguente dove sono riportate le seguenti informazioni:

Evento: Tipo di evento in corrispondenza del quale è previsto l'intervento formativo

Formazione: tipo di intervento formativo

Contenuti: contenuti dell'intervento formativo

**Tabella 6 - Regola 19.6 dell'allegato B - PIANIFICAZIONE INTERVENTI FORMATIVI**

<b>Evento</b>	<b>Formazione</b>	<b>Contenuti</b>
<i>Assunzione</i>	Generale	Informativa di tipo generale sull'utilizzo delle stazioni di lavoro e della rete
		Norme di utilizzo di Internet e della posta elettronica
		Criteri di scelta, utilizzo e conservazione delle password
	Applicativa	Norme di comportamento e di utilizzo specifiche a seconda dei trattamenti utilizzati
<i>Aggiornamento stazioni di lavoro</i>	Generale	Intervento formativo specifico sui nuovi strumenti hardware e software utilizzati
<i>Sostituzione o aggiornamento procedure applicative</i>	Applicativa	Intervento formativo sulle nuove caratteristiche dell'applicazione
<i>Modifica mansioni</i>	Applicativa	Intervento formativo sulle nuove applicazione che si andranno ad utilizzare

## Trattamenti affidati all'esterno (Regola 19.7)

In questa sezione sono descritti quei trattamenti relativi a dati personali oggetto di trattamento da parte dell'Ateneo e che sono affidati all'esterno. Tutti gli enti a cui sono affidati tali trattamenti rilasciano idonea dichiarazione di effettuare tali trattamenti esclusivamente per gli incarichi che sono stati affidati. Nella tabella 7 sono riportati i tipi di trattamenti, i dati interessati, l'ente incaricato ed la descrizione degli obiettivi per il quale il trattamento è affidato all'esterno. Da sottolineare il particolare rapporto che l'Ateneo ha con il Cineca che fornisce assistenza su tutte e tre le principali procedure di gestione amministrativa attualmente in esercizio e che, per scopi di



assistenza e verifica delle procedure stesse, effettua saltuariamente trattamenti dei dati elencati nella tabella.

**Tabella 7 - Regola 19.7 dell'Allegato B -TRATTAMENTI AFFIDATI ALL'ESTERNO**

<b>Descrizione attività</b>	<b>Trattamenti di dati interessati</b>	<b>Soggetto esterno</b>	<b>Descrizione dei criteri e degli impegni assunti</b>
Emissione bollettini pagamento rate tasse studentesche	Calcolo rata da pagare sulla base delle autocertificazioni	Ente tesoriere (Unicredito)	Emissione bollettini di pagamento e trasmissione dati dei pagamenti
Concessioni prestiti	Dati anagrafici e di carriera per il controllo dei requisiti	Banca Intesa	Emissione e pagamento rate finanziamenti sulla base delle indicazioni della Università
Assistenza procedura CSA	Dati del personale	CINECA	Controllo e verifica dei trattamenti in caso di malfunzionamenti e di aggiornamenti delle procedure
Assistenza procedura CIA	Dati personale e fornitori	CINECA	Controllo e verifica dei trattamenti in caso di malfunzionamenti e di aggiornamenti delle procedure
Assistenza procedura GISS	Dati studenti	CINECA	Controllo e verifica dei trattamenti in caso di malfunzionamenti e di aggiornamenti delle procedure



## **ALLEGATO A**

### **Schede analitiche Facoltà di Agraria**

Azienda agraria	Non pervenuto
Azienda Agraria - Rip. Tecnica	Non pervenuto
Centro Interdipartimentale Orto Botanico	Pervenuto (centro_ortobotanico)
Dipartimento di Scienze Ambientali e delle Produzioni Vegetali	Pervenuto(Dip_sc_amb)
Dipartimento di Scienze Applicate ai Sistemi Complessi	Non pervenuto
Dipartimento di Scienze degli Alimenti	Pervenuto (Dip_sc_alimenti)
Presidenza Facoltà di Agraria	Pervenuto (Pres_agraria)



**ALLEGATO B**

**Schede analitiche Facolta' di Economia**

Dipartimento di Economia  
Dipartimento di Scienze Sociali  
Dipartimento Management e Organizzazione Industriale  
Presidenza Facolta' di Economia

Pervenuto (Dip\_economia)  
Pervenuto (Dip\_sc\_sociali)  
Pervenuto (Dip\_management)  
Pervenuto (Pres\_economia)



## **ALLEGATO C**

### **Schede analitiche Facoltà di Ingegneria**

Dipartimento Architettura, Rilievo, Disegno, Urbanistica, Storia	Pervenuto (Dip_architettura)
Dipartimento di Architettura, Costruzioni e Strutture	Non pervenuto
Dipartimento di Elettromagnetismo e Bioingegneria	Pervenuto (Dip_elettro_bio)
Dipartimento di Elettronica, Intelligenza Artificiale e Telecomunicazioni	Pervenuto (Dip_elettro_iat)
Dipartimento di Energetica	Pervenuto (Dip_energetica) *
Dipartimento di Fisica e Ingegneria Materiali e Territorio	Non pervenuto
Dipartimento di Ingegneria Informatica, Gestionale e dell'Automazione	Pervenuto (Dip_ing_inf)
Dipartimento di Meccanica	Pervenuto (Dip_meccanica)
Dipartimento di Scienze Matematiche	Pervenuto (Dip_matematica)
Dipartimento Scienze dei Materiali e della Terra	Pervenuto (Dip_scienze_materiali)
Istituto di Idraulica e Infrastrutture viarie	Pervenuto (Ist_idraulica)
Presidenza Facoltà di Ingegneria	Non pervenuto



## **ALLEGATO D**

### **Schede analitiche Facoltà di Medicina**

Dipartimento di Neuroscienze	Pervenuto (Dip_neurosc)
Dipartimento di Patologia Molecolare e Terapie Innovative	Pervenuto (Dip_pat_mol)
Dipartimento di Scienze Mediche e Chirurgiche	Non pervenuto
Istituto Biotecnologie Biochimiche	Non pervenuto
Istituto di Biochimica	Non pervenuto
Istituto di Biologia e Genetica	Non pervenuto
Istituto di Malattie Infettive e Medicina Pubblica	Pervenuto (Ist_mal_infettive)
Istituto di Medicina Clinica e Biotecnologie Applicate	Non pervenuto
Istituto di Microbiologia e Scienze Biomediche	Non pervenuto
Istituto di Morfologia Umana Normale	Non pervenuto
Istituto di Radiologia	Non pervenuto
Istituto di Scienze Materno-Infantili	Non pervenuto
Istituto di Scienze Odontostomatologiche	Non pervenuto
Presidenza Facoltà di Medicina e Chirurgia	Pervenuto (Pres_medicina)



**ALLEGATO E**

**Schede analitiche Facoltà di Scienze**

Dipartimento Scienze del Mare  
Presidenza Facoltà di Scienze

Pervenuto (Dip\_sc\_mare)  
Pervenuto (Pres\_scienze)



**ALLEGATO F**

**Schede analitiche Centri**

Centro Ateneo di Documentazione  
Centro di Supporto per l'Apprendimento delle Lingue  
Centro Servizi Multimediali ed Informatici

Non pervenuto  
Pervenuto (Csal)  
Pervenuto (Cesmi)



**ALLEGATO G – DESCRIZIONE ANALITICA DELLE MISURE DI SICUREZZA**

**Regola 19.4 del Disciplinare Tecnico al D.Lgs. 163**

L'allegato è costituito da una scheda per ogni singola misura riportata nella Tabella 5 del Documento Programmatico sulla Sicurezza dell'Università Politecnica delle Marche



## **ALLEGATO G – Misura MIS001 – Gestione password Bios**

- Descrizione:** Attivazione della password del Bios sulla stazione di lavoro dell'incaricato
- Minaccia:** Accessi non autorizzati alla singola stazione di lavoro
- Tipologia:** Misura preventiva
- Responsabilità:** Questa singola misura pur essendo efficace può essere di intralcio all'operatività della singola stazione di lavoro. La responsabilità dell'adozione è lasciata al singolo incaricato che è adeguamento istruito sull'utilizzo della misura stessa, sugli effetti, sui vantaggi e sui rischi. Qualora la misura sia adottata, l'incaricato deve comunicare al proprio responsabile di riferimento la password adottata e le sue eventuali modifiche al fine di consentire l'accesso alla stazione di lavoro in caso di necessità. Le password sono mantenute in busta chiusa ed utilizzate in caso di necessità solo ed esclusivamente dietro autorizzazione del responsabile della struttura di riferimento
- Tempi:** Il tempo di validità di ogni singola password è determinato dall'incaricato, la password comunque deve essere rinnovata qualora si renda necessario l'accesso alla stazione di lavoro in assenza dell'incaricato stesso
- Ambiti:** L'applicazione di tale misura riguarda tutte le stazioni di lavoro che sono adibite al trattamento dei dati personali



## ALLEGATO G – Misura MIS002 – Gestione password dominio

- Descrizione:** La misura riguarda la gestione delle credenziali di accesso al dominio Windows e le politiche di validità delle stesse. Ogni incaricato che agisce all'interno della rete dell'Amministrazione Centrale per poter utilizzare la propria stazione di lavoro deve autenticarsi all'interno di un dominio Windows. Tale modalità sarà estesa anche a tutti gli incaricati dislocati nelle varie strutture periferiche. La credenziale di accesso è costituita da un nome utente unico e da una password la cui gestione segue le indicazioni sulle misure minime del D.Lgs. 163 ed in particolare: la password assegnata all'incaricato deve essere modificata al primo accesso al dominio, la sua lunghezza è di almeno 8 caratteri, ogni 6 mesi il sistema costringe alla modifica della password, se la stessa è inutilizzata o non è rinnovata alla scadenza le credenziali dell'incaricato sono automaticamente disabilitate
- Minaccia:** Accessi non autorizzati alla rete ed alle stazioni di lavoro
- Tipologia:** Misura preventiva
- Responsabilità:** La procedura di inizializzazione delle credenziali di accesso e configurazione del sistema per la loro gestione automatica in merito ai rinnovi, alle scadenze ed alle disabilitazioni sono a cura del Nucleo Informatico Amministrativo. La scelta delle singole password sono a carico del singolo incaricato.
- Tempi:** I tempi di validità sono automaticamente gestiti dal sistema rispettando le misure minime previste dal D.Lgs. 163
- Ambiti:** L'applicazione di tale misura riguarda al momento sono le stazioni di lavoro attestata sulla rete dell'Amministrazione Centrale ma saranno estese a tutta la rete di Ateneo nell'arco dei prossimi sei mesi



## **ALLEGATO G – Misura MIS003 – Gestione password trattamenti**

- Descrizione:** La misura riguarda l'accesso alle procedure relative ai diversi trattamenti descritti nella tabella 1 gestite direttamente dal Nucleo Informatico Amministrativo. Ad ogni utente di ogni procedura sono assegnate delle credenziali di accesso alla procedura stessa. Le credenziali sono costituite da un codice identificativo dell'incaricato (user name) e da una password. La password iniziale è comunicata per scritto in busta chiusa all'utente che al primo accesso alla procedura stessa è forzato alla modifica. Ogni password deve essere lunga almeno otto caratteri ed ha validità sei mesi dopodichè deve essere modificata a cura dell'utente stesso. Le credenziali sono modificate anche in presenza di smarrimento o di sottrazione delle stesse
- Minaccia:** Accessi non autorizzati alle procedure che mettono in essere i vari trattamenti
- Tipologia:** Misura di tipo preventivo e di contrasto nel caso di smarrimento delle credenziali
- Responsabilità:** La generazione delle password iniziali e della loro consegna è a cura del Nucleo Informatico Amministrativo. Il successivo aggiornamento delle password è a cura dei singoli titolari. Il Nucleo Informatico Amministrativo ha la responsabilità del controllo e del mantenimento delle varie procedure che automaticamente gestiscono l'aggiornamento e le scadenze delle credenziali di accesso dei singoli titolari
- Tempi:** La gestione delle password è in essere fino al mantenimento in esercizio di ogni singola procedura
- Ambiti:** Tale misura riguarda tutte le procedure descritte nella tabella 2 ad esclusione dei trattamenti gestiti direttamente da enti esterni



## **ALLEGATO G – MIS004 – Informativa utilizzo stazioni di lavoro**

- Descrizione:** Ad ogni incaricato sono impartite istruzioni relativamente ai rischi derivanti da un utilizzo non corretto delle stazioni di lavoro soprattutto per quanto riguarda la conservazione delle password di accesso alla rete ed alle procedure applicative oltre che a norme di comportamento in merito all'utilizzo di Internet e della posta elettronica
- Minaccia:** Disattenzione nell'utilizzo di strumenti informatici che possa arrecare danno alla rete come la diffusione di virus, di spyre, trojan ed altri eventi dannosi diffusi attraverso la rete
- Tipologia:** L'informativa è una misura tipicamente di tipo preventivo
- Responsabilità:** La responsabilità dell'informativa è del singolo responsabile coadiuvato dal Nucleo Informatico Amministrativo e successivamente del singolo incaricato nel rispettare le direttive ricevute
- Tempi:** L'attuazione è permanente in caso di nomina di nuovi incaricati o di nuove minacce che si possono presentare sulla rete
- Ambiti:** L'ambito di applicazione riguarda tutti gli incaricati che effettuano trattamenti con strumenti informatici collegati in rete e non



## **ALLEGATO G – Misura MIS005 – Aggiornamenti periodici sulle applicazioni**

- Descrizione:** Ad ogni incaricato ad un particolare trattamento sono impartite le istruzioni fondamentali nell'utilizzo della procedura con la quale si effettuano i trattamenti. Gli aggiornamenti sono periodici in corrispondenza di nuove funzionalità o nuove versioni delle procedure utilizzate
- Minaccia:** Utilizzo non corretto della procedure che possano causare la perdita o la incongruenza dei dati personali
- Tipologia:** Misura tipicamente preventiva ma anche di contrasto nel caso del verificarsi di malfunzionamenti o non corretti utilizzi delle varie procedure
- Responsabilità:** Le responsabilità degli aggiornamenti sono a carico dei responsabili nel decidere i momenti in cui tali aggiornamenti devono essere effettuati, a carico del Nucleo Informatico Amministrativo per quanto riguarda l'organizzazione e l'informazione in caso di nuove procedure o nuove versioni di procedure già in esercizio
- Tempi:** Misura permanente
- Ambiti:** Gli ambiti sono tipicamente applicativi e interessano tutti gli incaricati



## **ALLEGATO G – Misura MIS006 – Aggiornamento programmi antivirus**

- Descrizione:** La misura consiste nell'installazione e nella corretta configurazione di un programma antivirus su tutte le stazioni di lavoro al momento della loro consegna ai diversi responsabili e incaricati. Il programma antivirus è configurato per un aggiornamento giornaliero delle impronte virali mediante un collegamento ad uno dei server dislocati presso il Nucleo Informatico Amministrativo e nei vari Poli dell'Ateneo
- Minaccia:** Contrasto alla diffusione dei virus informatici
- Tipologia:** La misura è di tipo preventivo ma anche di contenimento degli effetti in caso di infezione di una stazione di lavoro
- Responsabilità:** L'installazione e la corretta configurazione sono a diretta responsabilità del Nucleo Informatico Amministrativo per le stazioni di lavoro acquistate e configurate direttamente dal personale del Nucleo, il mantenimento della configurazione è a carico del singolo incaricato
- Tempi:** La validità dell'antivirus è testata almeno una volta all'anno
- Ambiti:** Tutte le stazioni di lavoro attestate sulla rete e non



## **ALLEGATO G – Misura MIS007 – Aggiornamento attrezzature**

- Descrizione:** Aggiornamento periodico delle stazioni di lavoro assegnate agli incaricati per il trattamento dei dati. La sostituzione delle stazioni di lavoro avviene mediamente ogni 4 anni o in occasione di aggiornamenti delle procedure applicative o di sistema che richiedano una maggiore potenza di calcolo
- Minaccia:** Mantenere efficienti ed tecnologicamente adeguate le attrezzature informatiche consente di minimizzare i rischi dovuti a malfunzionamenti delle stesse e di prevenire la eventuale perdita di dati
- Tipologia:** La misura è tipicamente preventiva
- Responsabilità:** La responsabilità è del Nucleo Informatico Amministrativo e direttamente dell'incaricato del trattamento per quanto riguarda la segnalazione tempestiva di malfunzionamenti
- Tempi:** Annualmente si effettua una verifica delle attrezzature che hanno superato i tre anni di garanzia ed un controllo sulle funzionalità
- Ambiti:** Tutti i trattamenti



## **ALLEGATO G – Misura MIS008 – Firewall**

- Descrizione:** Un server dedicato con sistema operativo Linux svolge le funzioni di firewall per tutte le attrezzature di calcolo dislocate sulla rete della Amministrazione Centrale. Tale rete è suddivisa in una zona protetta all'interno della quale stanno tutte le macchine che non devono essere accessibili dall'esterno ed una zona libera all'interno della quale si trovano i server accessibili da internet.
- Minaccia:** Tentativi di accesso non autorizzato attraverso internet
- Tipologia:** Le misure di protezione del firewall sono di tipo preventivo ma anche di contrasto e contenimento
- Responsabilità:** La responsabilità della gestione e della corretta configurazione del firewall è a carico del Nucleo Informatico Amministrativo
- Tempi:** Le policies di sicurezza sono controllate e verificate ogni sei mesi
- Ambiti:** L'ambito di applicazione riguarda la rete della Amministrazione Centrale e quindi i tre edifici di Pizza Roma, Via Oberdan 8 e 12



## **ALLEGATO G – Misura MIS009 – Controllo accessi mediante smart card**

- Descrizione:** L'accesso ai locali della Amministrazione Centrale e dell'Ateneo in generale nelle ore in cui i locali stessi non sono presidiati dal personale di portineria sarà possibile mediante l'utilizzo di smart card assegnate ad ogni dipendente. Le stesse smart card saranno successivamente utilizzate da ogni incaricato per accedere alla propria stazione di lavoro in sostituzione delle credenziali di accesso utilizzate attualmente (MIS002)
- Minaccia:** Accessi non autorizzati ai locali dove sono dislocate le attrezzature di calcolo adibite al trattamento ed alla conservazione di dati personali
- Tipologia:** Preventiva e di contenimento
- Responsabilità:** Per quanto riguarda la gestione delle autorizzazioni per l'accesso agli edifici, la responsabilità è del Centro Sviluppo e Gestione Edilizia che ha in carico la manutenzione di tutti gli edifici
- Tempi:** La misura è permanente con revisione delle autorizzazioni a seconda delle diverse esigenze prospettate dai responsabili
- Ambiti:** Tutti gli edifici dell'Università Politecnica delle Marche



## **ALLEGATO G – Misura MIS010 – Conservazione copie**

- Descrizione:** La macchina che effettua le copie dei dati personali oggetto dei vari trattamenti è dislocata in ambiente diverso da quello in cui risiedono tutti gli archivi di produzione ed è mantenuta all'interno di un box a tenuta stagna e ignifugo
- Minaccia:** Eventi distruttivi che possono interessare i locali adibiti a sala macchine dove risiedono gli archivi dei dati personali
- Tipologia:** Misura di contrasto e contenimento degli effetti di eventuali eventi distruttivi che so verificassero
- Responsabilità:** Il mantenimento delle copie è a cura del Nucleo Informatico Amministrativo
- Tempi:** Validità fino al momento in cui non siano disponibili tecnologie più avanzate con un rapporto benefici/costo più elevato
- Ambiti:** Ambiti fisici relativi al locale adibito a sala macchine



## **ALLEGATO G – Misura MIS011 – Procedura crittografia**

- Descrizione:** La procedura consente di creare su un singolo personal computer un volume crittografato utilizzando diversi e i più diffusi algoritmi di crittografia. Ogni struttura che gestisce dati sensibili, ad esclusione di quelli gestiti con le diverse procedure centralizzate, sono dotate di tale procedura. Il volume di dati crittografati è creato e mantenuto da parte della struttura utilizzando una password a propria scelta
- Minaccia:** Protezione da accessi non autorizzati ai dati sensibili
- Tipologia:** Misura di contrasto e preventiva
- Responsabilità:** La scelta e la distribuzione della procedura e a diretta responsabilità della struttura che ha a sua volta la responsabilità di gestire i dati sensibili attraverso l'algoritmo di crittografia scelto
- Tempi:** Annualmente si procede ad una verifica della procedura in uso e ad una verifica dell'eventuale esistenza di procedure più efficienti
- Ambiti:** Tutti le stazioni di lavoro sulle quali sono mantenuti dati sensibili