Agenzia Regionale per l'Informatica e la Telematica		**Documento Programmatico sulla Sicurezza**		
Emesso da:	**A.R.I.T.**	*Codice documento* **DPS**	*Versione* **1.0**	*Data di emissione* **29/03/2012**

D.P.S.

Agenzia Regionale per l'Informatica e la Telematica

Via	**Via Napoli, 4 – 64019 Tortoreto Lido (TE)**
Tel/Fax	**086177101 / 08617710212**
C.F.	**91022630676**

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato (con o senza l'ausilio di strumenti elettronici) dall'Agenzia Regionale per l'Informatica e la Telematica, con sede a in Tortoreto Lido (TE), in Via Napoli 4 – 64019.

Indice

Indice generale

Premessa

Conformemente a quanto previsto dalla normativa nazionale in vigore, nello specifico a quanto disposto dall'Art. 34 e dall'Allegato B del Decreto Legislativo n. 196/2003 *"Codice in materia di protezione dei dati personali"*, nonchè nel rispetto dello schema di compilazione suggerito dal Garante, nel presente documento si forniscono adeguate informazioni riguardanti:

- l'elenco dei trattamenti dei dati personali (punto 19.1 del disciplinare), mediante:
  - l'individuazione dei tipi di dati personali trattati
  - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2 del disciplinare)
- l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare)
- le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati (punto 19.4 del disciplinare)
- i criteri e le modalità di ripristino dei dati in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare)
- la previsione di interventi formativi degli incaricati del trattamento (punto 19.6 del disciplinare)
- le procedure da seguire per il controllo sullo stato della sicurezza

Ambito applicativo

Il presente Documento Programmatico sulla Sicurezza, adottato dall'Agenzia Regionale per l'Informatica e la Telematica, con sede in Tortoreto Lido (TE), alla Via Napoli, 4 - 64019, definisce le politiche e gli standard di sicurezza in merito al complesso di operazioni, dalla stessa effettuate, relativamente al trattamento dei dati personali.

Nel seguito i termini Titolare, Responsabile, Incaricato e Dato personale sono usati in conformità alle definizioni del D. Lgs. 196/03.

Il presente Documento Programmatico Sulla Sicurezza (da ora in poi indicato come DPS) si applica per il trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Elenco dei trattamenti dei dati

L' Agenzia Regionale per l'Informatica e la Telematica, nella propria sede di Tortoreto Lido (TE), alla Via Napoli, 4 - 64019, procede al trattamento di dati personali, sensibili e giudiziari.

I trattamenti vengono effettuati solo ed esclusivamente per le attività strettamente necessarie allo svolgimento dei compiti istituzionali dell'Agenzia.

I dati personali vengono trattati solo da personale autorizzato e non vengono comunicati e/o diffusi a terzi.

I dati sensibili e giudiziari non vengono trattati tramite l'ausilio di strumenti elettronici.

TABELLE DEI TRATTAMENTI DEI DATI PERSONALI

Id.	T1
Descrizione sintetica	Gestione del personale (buste paga, archivio contratti, documenti inail e inps, assenze del personale, ferie, permessi)
Natura dei dati	Personali
Struttura di riferimento	Ufficio del Personale
Altre strutture	Ufficio Amministrazione, Ufficio Protocollo, Ufficio Contabilità
Strumenti utilizzati	PC, LAN, Protocollo Informatico, Software Office Automation, Software Team System Program
Banca dati	Planet Time Proietti s.n.c
Luogo di custodia dei supporti di memorizzazione	Ufficio del Personale.

Id.	T2
Descrizione sintetica	Certificati di malattia, Gestione archivio curriculum
Natura dei dati	Sensibili
Struttura di riferimento	Ufficio del Personale
Altre strutture	Ufficio Protocollo
Strumenti utilizzati	Archivio Cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Armadio dotato di serratura dell'Ufficio del Personale

Id.	T3
Descrizione sintetica	Archivio Indirizzi Email

Natura dei dati	Personali
Struttura di riferimento	Ufficio Area Tecnica 9
Altre strutture	
Strumenti utilizzati	PC, LAN, Software Office Automation
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Area Tecnica 9

Id.	T4
Descrizione sintetica	Gestione Contabile (inserimento fatture, elaborazione mandati e reversali, bilancio, predisposizione atti liquidazione, predisposizione atti amministrativi)
Natura dei dati	Personali
Struttura di riferimento	Ufficio Contabilità
Altre strutture	
Strumenti utilizzati	PC, LAN, Protocollo Informatico, Software Office Automation, Software Target Cross
Banca dati	Target Cross, Archivio Cartaceo
Luogo di custodia dei supporti di memorizzazione	Sala Server 2P (archivio informatico); Armadio dotato di serratura dell' Ufficio Contabilità (archivio cartaceo);

Id.	T5
Descrizione sintetica	Assegnazione attrezzature informatiche ai collaboratori, consulenti e dipendenti
Natura dei dati	Personali
Struttura di riferimento	Ufficio Area Tecnica 9
Altre strutture	

Strumenti utilizzati	PC, LAN, Software Office Automation
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Area Tecnica 9

Id.	T6
Descrizione sintetica	Backup dati LAN ARIT e LAN AMMINISTRAZIONE
Natura dei dati	Personali
Struttura di riferimento	Ufficio Area Tecnica 9
Altre strutture	
Strumenti utilizzati	PC, LAN, Software di Network Backup, DAT
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Cassaforte presso Ufficio Area Tecnica 10

Id.	T7
Descrizione sintetica	Trattamento dei dati personali, relative a persona giuridiche, fisiche, Enti, concernenti ogni fase del pre-gara, gara e post-gara, stipula contratti e di atti amministrativi di competenza.
Natura dei dati	Personali
Struttura di riferimento	Ufficio Legale, Appalti&Contratti, Segreteria Tecnica;
Altre strutture	Ufficio Amministrazione, Ufficio Protocollo, Ufficio Contabilità
Strumenti utilizzati	PC, LAN, Protocollo informatico, Software Office Automation
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Legale, Appalti&Contratti, Segreteria Tecnica;

Id.	T8
Descrizione sintetica	Trattamento dei dati personali, relative a persona giuridiche, fisiche, Enti, concernenti ogni fase del pre-gara, gara e post-gara, stipula contratti e di atti atti amministrativi di competenza.
Natura dei dati	Giudiziari
Struttura di riferimento	Ufficio Legale, Appalti&Contratti, Segreteria Tecnica;
Altre strutture	Uffici Amministrazione, Ufficio Protocollo
Strumenti utilizzati	Archivio Cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Armadio dotato di serratura dell' Ufficio Legale, Appalti&Contratti, Segreteria Tecnica

Id.	T9
Descrizione sintetica	Gestione Protocollo
Natura dei dati	Personali
Struttura di riferimento	Ufficio Protocollo
Altre strutture	Ufficio del Personale, Ufficio Contabilità
Strumenti utilizzati	PC, LAN, Protocollo Informatico, Software Office Automation
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Protocollo

Id.	T10
Descrizione sintetica	Gestione Protocollo
Natura dei dati	Sensibili, Giudiziari
Struttura di riferimento	Ufficio Protocollo
Altre strutture	Ufficio del Personale
Strumenti utilizzati	Archivio Cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Armadio dotato di serratura dell' Ufficio Protocollo

Id.	T11
Descrizione sintetica	Predisposizione Atti Amministrativi, Archivio Atti, Corrispondenza
Natura dei dati	Personali
Struttura di riferimento	Ufficio Amministrazione
Altre strutture	
Strumenti utilizzati	PC, LAN, Protocollo Informatico, Software Office Automation
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Amministrazione

Id.	T12
Descrizione sintetica	Predisposizione Atti Amministrativi, Archivio Atti, Corrispondenza
Natura dei dati	Sensibili, Giudiziari
Struttura di riferimento	Ufficio Amministrazione

Altre strutture	
Strumenti utilizzati	Archivio Cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Armadio dotato di serratura dell' Ufficio Amministrazione

Id.	T13
Descrizione sintetica	Predisposizione Atti, Contratti, Delibere
Natura dei dati	Personali
Struttura di riferimento	Ufficio Segreteria Direzione
Altre strutture	Ufficio Amministrazione, Ufficio Protocollo, Ufficio del Personale
Strumenti utilizzati	PC, LAN, Protocollo Informatico, Software Office Automation, Archivio cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Segreteria Direzione; Armadio dotato di serratura dell' Ufficio Segreteria Direzione (archivio cartaceo)

Id.	T14
Descrizione sintetica	Dati personali di aziende, collaboratori e professionisti per rendicontazione e monitoraggio progetti
Natura dei dati	Personali
Struttura di riferimento	Ufficio Monitoraggio & Rendicontazione
Altre strutture	
Strumenti utilizzati	PC, LAN, Software Office Automation, Software Target Cross
Banca dati	Target Cross
Luogo di custodia	Sala Server 2P

dei supporti di memorizzazione	

Id.	T15
Descrizione sintetica	Archivio ingresso/uscita persone, Rubrica Telefonica
Natura dei dati	Personali
Struttura di riferimento	Ufficio Reception
Altre strutture	
Strumenti utilizzati	Archivio Cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Ufficio Reception

Id.	T16
Descrizione sintetica	Attività di accesso agli atti
Natura dei dati	Personali, Giudiziari
Struttura di riferimento	Ufficio Legale, Appalti&Contratti, Segreteria Tecnica;
Altre strutture	
Strumenti utilizzati	Archivio Cartaceo
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Armadio dotato di serratura dell'Ufficio Legale, Appalti&Contratti, Segreteria Tecnica

Id.	T17
Descrizione sintetica	Trattamento di dati relativi alle persone fisiche, giuridiche e società esterne relativi alla gestione dei Progetti ARIT

Natura dei dati	Personali
Struttura di riferimento	Uffici Area Tecnica;
Altre strutture	
Strumenti utilizzati	PC, LAN, Software Office Automation
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Uffici Area Tecnica; Ufficio Monitoraggio & Rendicontazione; Ufficio Legale, Appalti&Contratti, Segreteria Tecnica;

Id.	T18
Descrizione sintetica	Trattamento di dati relativi a tutti gli atti amministrativi ARIT, inclusi gli atti derivanti dall'attività amministrativa.
Natura dei dati	Personali
Struttura di riferimento	Uffici Direzione Amministrativa;
Altre strutture	
Strumenti utilizzati	PC, LAN, Software Office Automation, Archivi Cartacei
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Uffici Direzione Amministrativa; Ufficio Amministrazione; Ufficio Protocollo; Ufficio del Personale; Ufficio Contabilità; Ufficio Segreteria Direzione

Id.	T19
Descrizione sintetica	Trattamento di dati relativi alle password.
Natura dei dati	Tutti
Struttura di riferimento	Direzione Generale;
Altre strutture	
Strumenti utilizzati	Archivi Cartacei
Banca dati	
Luogo di custodia dei supporti di memorizzazione	Uffici Direzione Generale

Distribuzione dei compiti e delle responsabilità

All'interno dell'ARIT sono preposti al trattamento dei dati personali i seguenti uffici (vedi All. A – Pianta Edificio):

- Ufficio Area Tecnica N (N = 1,2,3,4,6,7,8,9,10)
- Ufficio Monitoraggio & Rendicontazione
- Ufficio Legale, Appalti&Contratti, Segreteria Tecnica
- Ufficio Contabilità
- Ufficio del Personale
- Ufficio Amministrazione
- Ufficio Protocollo
- Ufficio Segreteria Direzione
- Ufficio Reception

Il personale dell'ARIT è organizzato a livello logico conformemente a quanto illustrato nell'organigramma allegato al presente documento. (vedi All. I – Organigramma Logico Privacy). L'occupazione fisica dei locali da parte del personale rispecchia la situazione al momento della stesura del presente documento.

L'Ufficio Area Tecnica N procedono ai trattamenti identificati dai seguenti codici T3, T5, T6 e T17 ed sono composti dalle seguenti persone:

- Sig. *Donato Colangelo* – Dipendente – Autorizzato ad accedere agli archivi elettronici relativi ai trattamenti T3, T5, T6 e T17, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso;
- *Dr. Gianluca Del Conte* – Dipendente - Autorizzato ad accedere agli archivi elettronici relativi ai trattamenti T3, T5, T6 e T17, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso;

- Dott. *Alessio Albani,* Ing. *Ludovica Collacciani*, Ing. *Pier Daniele Cretara*, Ing. *Roberto Di Lorenzo*, Ing. *Domenico Di Martino*, Sig. *Giuseppe Ferrante*, Ing. *Laura Fuciarelli*, Ing. *Fabio Goderecci*, Ing. *Alfonso Ponziani,* Ing. *Massimiliano De Sanctis, Arch. Luciano Matani, Ing. Carlo Iachini* - Dipendenti a Tempo Determinato - Autorizzati ad accedere agli archivi elettronici relativi ai trattamenti T17, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso;

L'Ufficio Legale, Appalti&Contratti, Segreteria Tecnica procede ai trattamenti identificati dai seguenti codici T7, T8, T16, e T17 ed è composto dalle seguenti persone:

- Dott.ssa *Stefania Trapanese*, Dott.ssa *Eugenia Tassoni*, Dott.ssa *Claudia Valsesia* - Dipendenti - Autorizzati ad accedere agli archivi cartacei ed elettronici relativi ai trattamenti T7, T8, T16, e T17, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso;

L'Ufficio Monitoraggio & Rendicontazione procede ai trattamenti identificati dai seguenti codici T14 e T17 ed è composto dalle seguenti persone:

- Dott. *Domenico Lilla*, Sig. *Serpenti Fabrizo* - Dipendenti - Autorizzati ad accedere agli archivi elettronici relativi ai trattamenti T14 e T17, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso;

L'Ufficio Contabilità procede ai trattamenti identificati dal codice T1, T4, T7 e T9 ed è composto dalle seguenti persone:

- Sig. *Pietro Ricci*, Dott.ssa *Monica Tassoni* - Dipendenti – Autorizzati ad accedere agli archivi cartacei ed elettronici relativi al trattamento T1, T4, T7 e T9, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso.

L'Ufficio del Personale procede ai trattamenti identificati dai seguenti codici T1, T2, T9, T10 e T13 ed è composto dalle seguenti persone:

- *Dott. Severino Marcelli, Sig. Pietro Ricci-* Dipendente – Autorizzato ad accedere agli archivi cartacei ed elettronici relativi ai trattamenti T1, T2, T9, T10 e T13, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso.
- *Società TINN S.r.l.* – Outsourcing – Autorizzata ad accedere agli archivi cartacei ed elettronici relativi ai trattamenti T1, T2, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia del Grosso. (La società TINN S.r.l. con sede legale in via Po, 12 Teramo, ha ricevuto tale incarico attraverso la delibera N° 4 del 23 Gennaio 2012, inerente l'affidamento della fornitura del servizio in outsourcing della gestione economica del personale dell'Arit).

L'Ufficio Amministrazione procede ai trattamenti identificati dai seguenti codici T1, T7, T8, T11, T12, e T13 ed è composto dalle seguenti persone:

- Dott. *Severino Marcelli* - Dipendente - Autorizzato ad accedere agli archivi cartacei ed elettronici relativi ai trattamenti T1, T7, T8, T11, T12, e T13, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso.

L'Ufficio Protocollo procede ai trattamenti identificati dai seguenti codici T1, T2, T7, T8, T9, T10 e T13 ed è composto dalle seguenti persone:

- Dott. *Severino Marcelli* - Dipendente - Autorizzato ad accedere agli archivi cartacei ed elettronici relativi ai trattamenti T1, T2, T7, T8, T9, T10 e T13, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso.

L'Ufficio Segreteria di Direzione procede ai trattamenti identificati dal codice T13 ed è composto dalle seguenti persone:

- *Sig.ra Federica De Iulis* - Dipendente - Autorizzata ad accedere agli archivi cartacei ed elettronici relativi al trattamento T13, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso.

L'Ufficio Reception procede ai trattamenti identificati dal codice T15 ed è composto dalle seguenti persone:

- Sig.ra *Simona Luciani*, Sig. *Giuseppe Giansante*, Sig.ra *Federica Maiorani* - Collaboratori – Autorizzati ad accedere agli archivi cartacei ed elettronici relativi ai trattamenti T15, sotto la direzione e la responsabilità del Responsabile del Trattamento Dott.ssa Lucia Del Grosso;

Analisi dei rischi che incombono sui dati

La seguente tabella elenca le possibili tipologie di rischio a cui sono soggetti i dati.

ID Rischio	Descrizione
R1	Sottrazione credenziali di autenticazione
R2	Carenza di consapevolezza, disattenzione o incuria
R3	Azione di virus informatici o di programmi suscettibili di recare danno
R4	Malfunzionamento, indisponibilità o degrado degli strumenti
R5	Accessi esterni non autorizzati
R6	Intercettazione di informazioni di rete
R7	Accessi non autorizzati a locali/reparti ad accesso ristretto
R8	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi)
R9	Guasto a sistemi complementari (impianto elettrico/climatizzazione)
R10	Errori umani nella gestione della sicurezza

Misure in essere e da adottare

Per ogni rischio individuato al paragrafo precedente segue:

1) una descrizione delle misure adottate per contrastare tale rischio;
2) le eventuali misure da adottare;
3) le attività periodiche di verifica e controllo, essenziali per assicurarne l'efficacia.

L'ARIT si è munita di un regolamento interno (All. H - Norme Tecniche) che disciplina le linee guida generali per la configurazione/manutenzione delle attrezzature informatiche da adottare a cura del personale dell'Area Tecnica.

ID Misura	M1
Rischi contrastati	R1,R5
Trattamenti Interessati	
Misure già in essere	L'accesso ai computer connessi alla LAN ARIT (vedi All. B – Schema di Rete) avviene per mezzo di un meccanismo di autenticazione centralizzata. In particolare all'interno della LAN ARIT è presente un server nel quale è installato il sistema operativo Microsoft Windows 2000 che assolve alla funzione di controller di dominio (DC d'ora in poi). Per ogni utente che impiega un computer connesso alla LAN ARIT, è configurato un profilo personale nel DC che permette l'accesso alle risorse di calcolo tramite le credenziali di autenticazione (nome utente e password). I profili sono configurati in maniera tale da: • obbligare gli utenti ad eseguire il cambio della password ogni 6 mesi • rifiutare le password composte da un numero di caratteri inferiori a 8 Per ogni nuovo profilo creato, viene impostato il cambio

	obbligatorio della password al primo accesso. Ciò permette di garantire che la password sia conosciuta solo ed esclusivamente dall'utente assegnatario del profilo. Questo procedimento permette di evitare la necessità di mantenere archivi contenenti le credenziali di autenticazione e pertanto riduce i rischi relativi alla loro sottrazione. Le password di amministrazione di tutti i sistemi informatici ARIT sono scritte e conservate all'interno di buste chiuse e siglate dal responsabile della password presso la cassaforte dell'Ufficio della Direzione Generale al secondo piano. Le eventuali password di cartelle e file sono scritte e conservate all'interno di buste chiuse e siglate dal responsabile della password presso la cassaforte dell'Ufficio della Direzione Generale al secondo piano.
Misure da adottare	
Attività periodiche	
Strutture o persone addette all'adozione	Tutti i dipendenti, collaboratori e consulenti che abbiano ricevuto in dotazione un computer.

ID Misura	M2
Rischi contrastati	R1,R2,R3,R4,R5
Trattamenti Interessati	
Misure già in essere	I dipendenti, i collaboratori e i consulenti sono stati informati (tramite circolare interna vedi All. C – Norme d'uso delle attrezzature informatiche ARIT) in merito alle norme d'uso delle risorse informatiche e telematiche. Tale normativa è rivolta a responsabilizzare gli utenti al fine di garantire: • la massima efficienza delle risorse di calcolo • la riservatezza e la sicurezza delle informazioni e dei dati • l'omogeneità sulle modalità operative di utilizzo delle apparecchiature
Misure da adottare	Corso di formazione in materia di privacy al fine di sensibilizzare i responsabili e gli incaricati relativamente ai rischi ed alle

	responsabilità civili e penali derivanti dal trattamento di dati personali, giudiziari e sensibili.
Attività periodiche	
Strutture o persone addette all'adozione	Tutti i dipendenti, collaboratori e consulenti che abbiano ricevuto in dotazione un computer.

ID Misura	M3
Rischi contrastati	R3,R4,R5
Trattamenti Interessati	
Misure già in essere	All'interno della LAN ARIT è presente un server nel quale è stato installato un software Antivirus basato su architettura Client/Server. Il software Antivirus implementa due funzionalità principali: • download automatico degli aggiornamenti delle definizioni dei virus. Una volta completato il download, gli aggiornamenti vengono automaticamente distribuiti ai client. • monitoring dello stato dei client: se un client non è aggiornato con l'ultima versione disponibile di definizione di virus o se si è verificata un'infezione, il software di gestione, della componente Server dell'Antivirus, è in grado di riportare tali anomalie. In ogni computer collegato alla rete LAN ARIT o alla rete LAN AMMINISTRAZIONE (vedi All. B – Schema di rete) è installato la componente client del software Antivirus.
Misure da adottare	
Attività periodiche	Il personale dell'area tecnica si impegna nell'attività costante di controllo/rimozione di software spyware accidentalmente installato nei PC.
Strutture o persone	Area Tecnica

addette all'adozione	

ID Misura	M4
Rischi contrastati	R3, R4
Trattamenti Interessati	
Misure già in essere	L'ARIT ha provveduto all'implementazione di opportune politiche di backup al fine di garantire la disponibilità dei dati nonchè la possibilità di ripristino in tempi ragionevoli. La metodologia di backup che è stata adottata è organizzata su più livelli: • i dati presenti nella cartella Documenti e nell'area Desktop di ogni utente della LAN ARIT, a cui è stato assegnato un profilo nel DC, vengono salvati nel server DC al momento dell'arresto del sistema operativo; • i dati raccolti dal server DC costituiscono la copia speculare di ciò che è presente al momento dell'arresto del sistema nella cartella Documenti e nell'area Desktop dei computer degli utenti. Questo significa che se un utente elimina un file dal proprio computer non ne viene conservata memoria storica nel DC. Per ovviare a tale problema è stato adottato un software di backup che con cadenza giornaliera esegue il backup dei dati contenuti nel DC all'interno di una unità di Storage IBM configurata in modalità Raid-5. Anche per i dati presenti nel server Contabilità della LAN AMMINISTRAZIONE viene eseguito un backup utilizzando come supporto di memorizzazione l'unità di storage IBM; • con cadenza mensile viene eseguita una copia di sicurezza su tape magnetico dei dati archiviati all'interno dell'unità di

	storage IBM. Il tape magnetico viene conservato all'interno della cassaforte presso l'ufficio Contact Center. Le chiavi della Cassaforte vengono conservate presso la Reception; il personale della Reception è stato informato tramite comunicazione interna prot. xyz (vedi All. D - Gestione chiavi cassaforte 1° Piano) riguardo le modalità operative e le autorizzazioni per la consegna delle chiavi della cassaforte.
Misure da adottare	
Attività periodiche	Il sig. Donato Colangelo si impegna ad eseguire con cadenza mensile una copia di sicurezza su tape magnetico dei dati archiviati all'interno dell'unità di storage IBM. Il sig. Donato Colangelo si impegna altresì ad eseguire con cadenza mensile un test di ripristino su un campione casuale di dati al fine di verificare l'efficacia del sistema di backup.
Strutture o persone addette all'adozione	Area Tecnica

ID Misura	M5
Rischi contrastati	R5,R6
Trattamenti Interessati	
Misure già in essere	L'infrastruttura di rete ARIT è composta da 7 reti: LAN ARIT, BACKEND, DMZ, LAN TEMP, WIRELESS, COLLABORATORI, LAN AMMINISTRAZIONE (vedi All. B – Schema di Rete). Un Firewall centralizzato gestisce tutte le politiche di traffico fra le varie reti impedendo così accessi non autorizzati sia dalla rete Internet che dalle reti interne. Si è prestata particolare attenzione alla protezione della rete LAN ARIT, implementando politiche di filtro del traffico a livello di protocolli di comunicazione e di indirizzi IP.

	La rete LAN AMMINISTRAZIONE è stata isolata fisicamente dalle altre reti impedendone l'accesso alla rete Internet o a qualsiasi altra rete interna: questo approccio permette di minimizzare le probabilità di accessi non autorizzati o di intercettazione del traffico di rete, garantendo quindi una livello di sicurezza maggiore per i dati gestiti dai computer afferenti alla LAN AMMINISTRAZIONE.
Misure da adottare	
Attività periodiche	Verifica periodica delle vulnerabilità tramite l'impiego di software per l'auditing di rete.
Strutture o persone addette all'adozione	Area Tecnica

ID Misura	M6
Rischi contrastati	R7
Trattamenti Interessati	
Misure già in essere	L'accesso a tutti i locali ARIT (vedi All. A - Pianta Edificio) avviene per mezzo di porte dotate di serratura. Tutte le chiavi necessarie per l'apertura/chiusura delle serrature in questione sono conservate presso l'ufficio Reception. Il personale dell'ufficio Reception è stato istruito mediante comunicazione interna (vedi All. E - Modalità accesso sala server 1P, All. F - Modalità accesso sala server 2P, All. G - Modalità accesso Uffici) sulle modalità operative e sulle autorizzazioni per l'accesso ai locali.
Misure da adottare	Dotare i locali della sala server al piano 1° e 2° di serrature elettroniche.
Attività periodiche	
Strutture o persone addette all'adozione	Reception

ID Misura	M7
Rischi contrastati	R8
Trattamenti Interessati	
Misure già in essere	L'ARIT è dotata di un sistema di allarme per la rilevazione degli incendi. Nella piantina (vedi All. A - Pianta Edificio) viene evidenziata la disposizione dei rilevatori di fumo all'interno dei locali. In ogni piano sono presenti almeno 2 estintori.
Misure da adottare	
Attività periodiche	Verifica stato estintori
Strutture o persone addette all'adozione	Area Tecnica, Personale esterno per manutenzione/verifica

ID Misura	M8
Rischi contrastati	R9
Trattamenti Interessati	
Misure già in essere	Per fronteggiare i casi di guasto, indisponibilità o black out dell'impianto di alimentazione elettrica, l'ARIT si è dotata di sistemi UPS (gruppi di continuità). Tali sistemi garantiscono l'alimentazione elettrica all'intera struttura per un tempo massimo di 3 ore. In caso di guasto agli impianti di climatizzazione delle sale server, sono state predisposte opportune procedure di spegnimento degli apparti hardware (vedi All. F - Modalità accesso sala server 2P) al fine di evitare eventuali danneggiamenti degli stessi. La temperatura del locale Sala Server 2 viene monitorata, per mezzo di una videocamera, dal personale dell'Area Tecnica e della Reception, permettendo così la rilevazione tempestiva di una possibile anomalia.
Misure da adottare	Collegare i condizionatori della sala server al 2° piano all'impianto UPS.
Attività periodiche	Verifiche dell'impianto UPS
Strutture o persone addette all'adozione	

Criteri e modalità di ripristino della disponibilità dei dati

Come già anticipato nel paragrafo precedente (tabella Misura M4), l'ARIT ha posto in essere opportune politiche di gestione dei backup per far fronte alle possibili minacce che possono comportare la perdita o il danneggiamento dei dati.
Nell'infrastruttura di rete ARIT sono presenti due reti di particolare importanza (vedi All. B - Schema di Rete Generale):

- LAN ARIT
- LAN AMMINISTRAZIONE

Queste sono le due reti che connettono gli elaboratori tramite i quali gli incaricati eseguono i trattamenti elencati al paragrafo 2.

Backup LAN ARIT

Tutti gli utenti che utilizzano computer connessi alla rete LAN ARIT e che effettuano almeno uno dei trattamenti elencati al paragrafo 2, hanno un profilo utente nel Dominio Arit gestito dal server Domain Controller (vedi All. B - Schema di Rete Lan Arit).
Tale profilo è creato al fine di consentire l'autenticazione e l'accesso alle risorse dell'elaboratore.
Gli utenti sono stati istruiti mediante circolare interna (vedi All. C – Norme d'uso delle attrezzature informatiche ARIT), sulle modalità di utilizzo delle attrezzature informatiche ARIT e in particolare sulla locazione fisica nella quale devono risiedere tutti i dati soggetti a trattamento:

"Ogni utente deve strutturare la cartella "Documenti" in "ARIT_NomeUtente" che deve essere costituita a sua volta dalle cartelle "Documenti_Definitivi" e "Documenti_Provvisori". Tutta la documentazione prodotta con qualsiasi strumento o sistema operativo, deve essere archiviata nelle cartelle suddette."

Questa politica di organizzazione dati è particolarmente utile ai fini della gestione del backup; infatti (per gli utenti che hanno associato un profilo nel Dominio Arit) all'atto di spegnimento del computer, tutti i dati presenti in quel momento nella cartella Documenti e nell'Area Desktop vengono copiati nel server Domain Controller, implementando quindi un primo livello di backup dei dati trattati.
Questo approccio è comunque limitativo in quanto ciò che viene conservato nel server Domain Controller, è esattamente la copia speculare di ciò che è presente nei computer degli utenti, impedendo quindi di mantenere una memoria storica nel tempo dei dati trattati.
Per ovviare a tale problema è stato implementato un sistema di Network Backup che permette di centralizzare i backup verso un vero e proprio backup server. Tale server è equipaggiato con una unità di Storage IBM Exp 300 composta da 12 dischi SCSI configurati in modalità RAID-5.
Il sistema è programmato per eseguire quotidianamente il backup incrementale dei dati presenti nel Domain Controller, mentre il primo giorno di ogni mese il backup viene eseguito in modalità Full.

Backup LAN AMMINISTRAZIONE

Nella rete LAN AMMINISTRAZIONE non è presente un Domain Controller. Gli utenti che usano computer connessi a questa rete sono stati istruiti mediante circolare interna (vedi All. C – Norme d'uso delle attrezzature informatiche ARIT) sulle modalità di utilizzo delle attrezzature informatiche ARIT e in particolare sulla locazione fisica nella quale devono risiedere tutti i dati trattati:

"Ogni utente deve strutturare la cartella "Documenti" in "ARIT_NomeUtente" che deve essere costituita a sua volta dalle cartelle "Documenti_Definitivi" e "Documenti_Provvisori". Tutta la documentazione prodotta con qualsiasi strumento o sistema operativo, deve essere archiviata nelle cartelle suddette.

Per gli utenti i cui computer sono connessi alla rete LAN AMMINISTRAZIONE valgono le stesse istruzioni sopra riportate ad eccezione per il fatto che per cartella Documenti si intende la cartella personale presente nel server Contabilità (configurata dal personale dell'Area Tecnica per ogni utente) a cui è possibile accedere tramite apposito Collegamento su Desktop. Qualora ci fossero incertezze relative alla connessione alla LAN AMMINISTRAZIONE oppure alla possibilità di accesso alla propria Cartella personale si prega di voler contattare il personale dell'Area Tecnica"

Anche per il backup dei dati della LAN AMMINISTRAZIONE viene utilizzato il sistema di Network Backup che preleva i dati da salvare direttamente dal server Contabilità e li trasferisce nell'unità di Storage IBM.
Il sistema è programmato per eseguire quotidianamente il backup incrementale dei dati presenti nel server Contabilità, mentre il primo giorno di ogni mese il backup viene eseguito in modalità Full.

Backup di Sicurezza

Entro i primi 5 giorni di ogni mese, il Sig. Donato Colangelo si impegna ad eseguire il ripristino di tutti i dati salvati nel sistema di Network Backup archiviati alla data dell'ultimo giorno del mese precedente.
I dati ripristinati vengono memorizzati su un tape magnetico. Il tape magnetico viene conservato all'interno della cassaforte presso l'Ufficio Area Tecnica N° 10 (vedi All. A - Pianta Edificio Piano 1).
Le chiavi per l'accesso alla Cassaforte vengono conservate presso la Reception; il personale della Reception è stato informato tramite comunicazione interna (All. D – Gestione chiavi cassaforte 1° Piano) riguardo le modalità operative e le autorizzazioni per la consegna delle chiavi della cassaforte.

Test di ripristino

Entro i primi 5 giorni di ogni mese e solo dopo aver eseguito il Backup di Sicurezza, il Sig. Donato Colangelo si impegna ad eseguire un test di ripristino dei dati secondo le seguenti modalità:

- vengono prelevati gli ultimi due tape magnetici in ordine cronologico di archiviazione;
- per ogni tape viene scelto un campione casuale di dati da ripristinare;
- viene eseguita la procedura di ripristino verificando il buon esito dell'operazione.

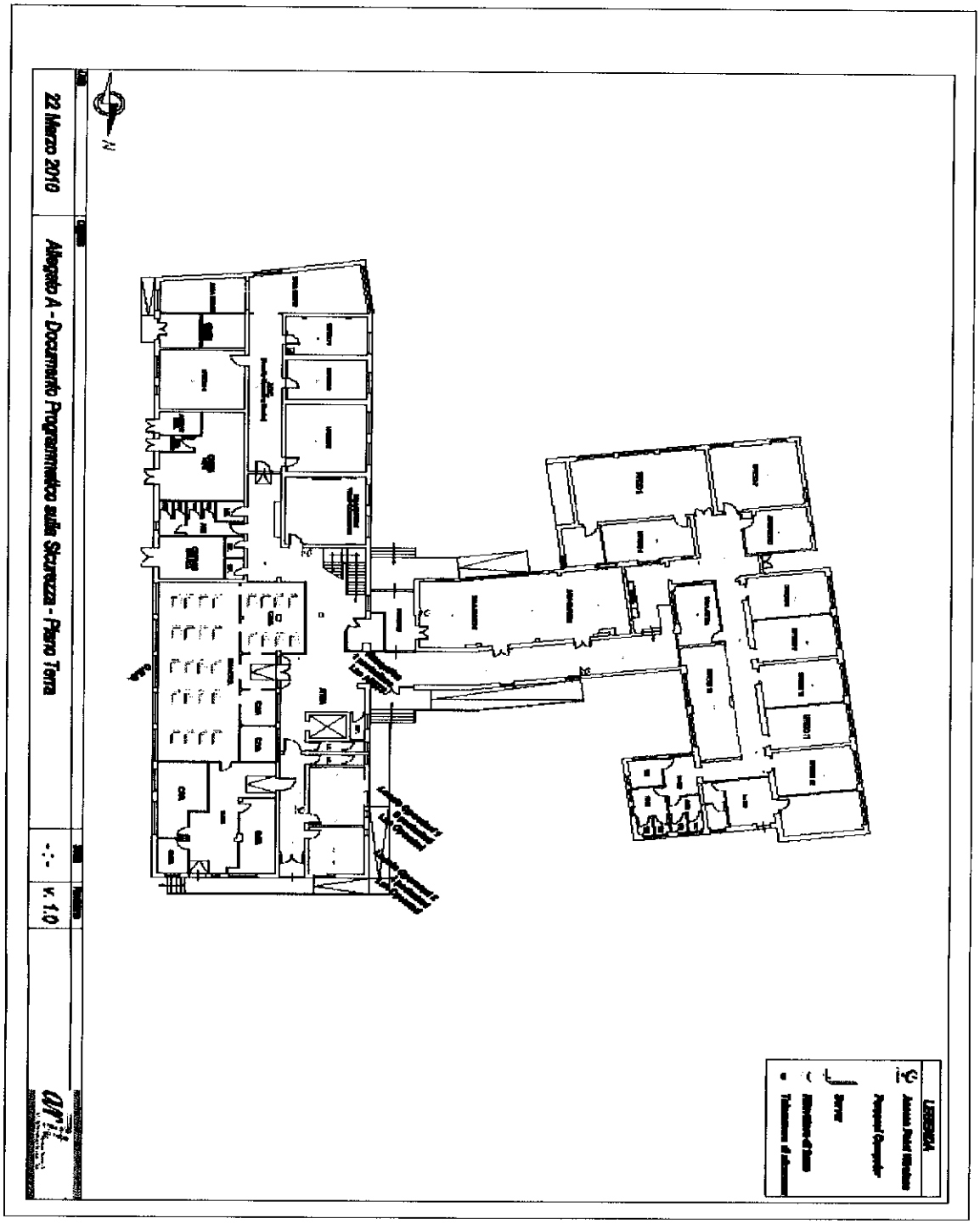
Pianificazione degli interventi formativi effettuati

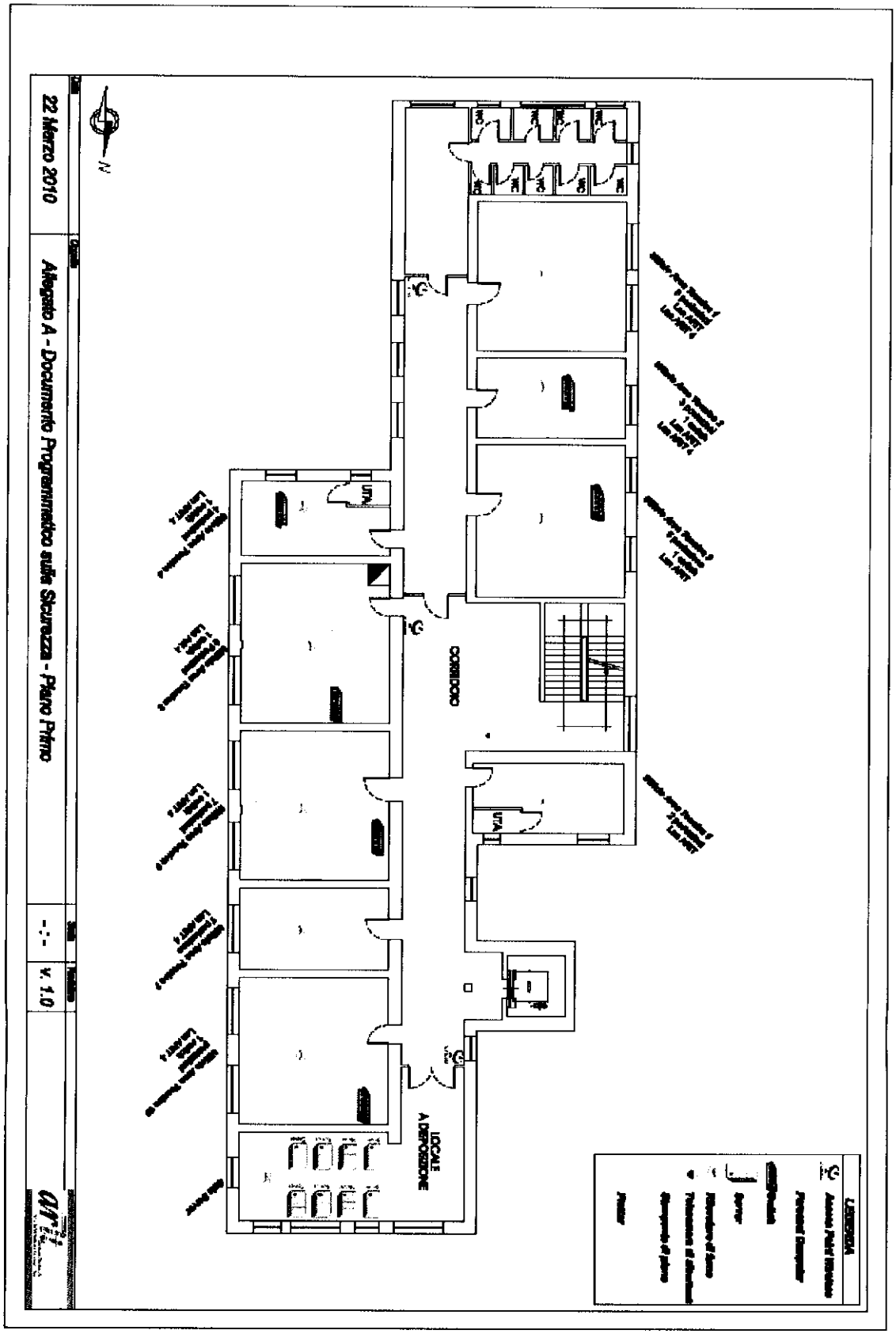
A seguito dell'attuazione del DPS, i dipendenti, i collaboratori e i consulenti ARIT sono stati informati ed istruiti in merito:

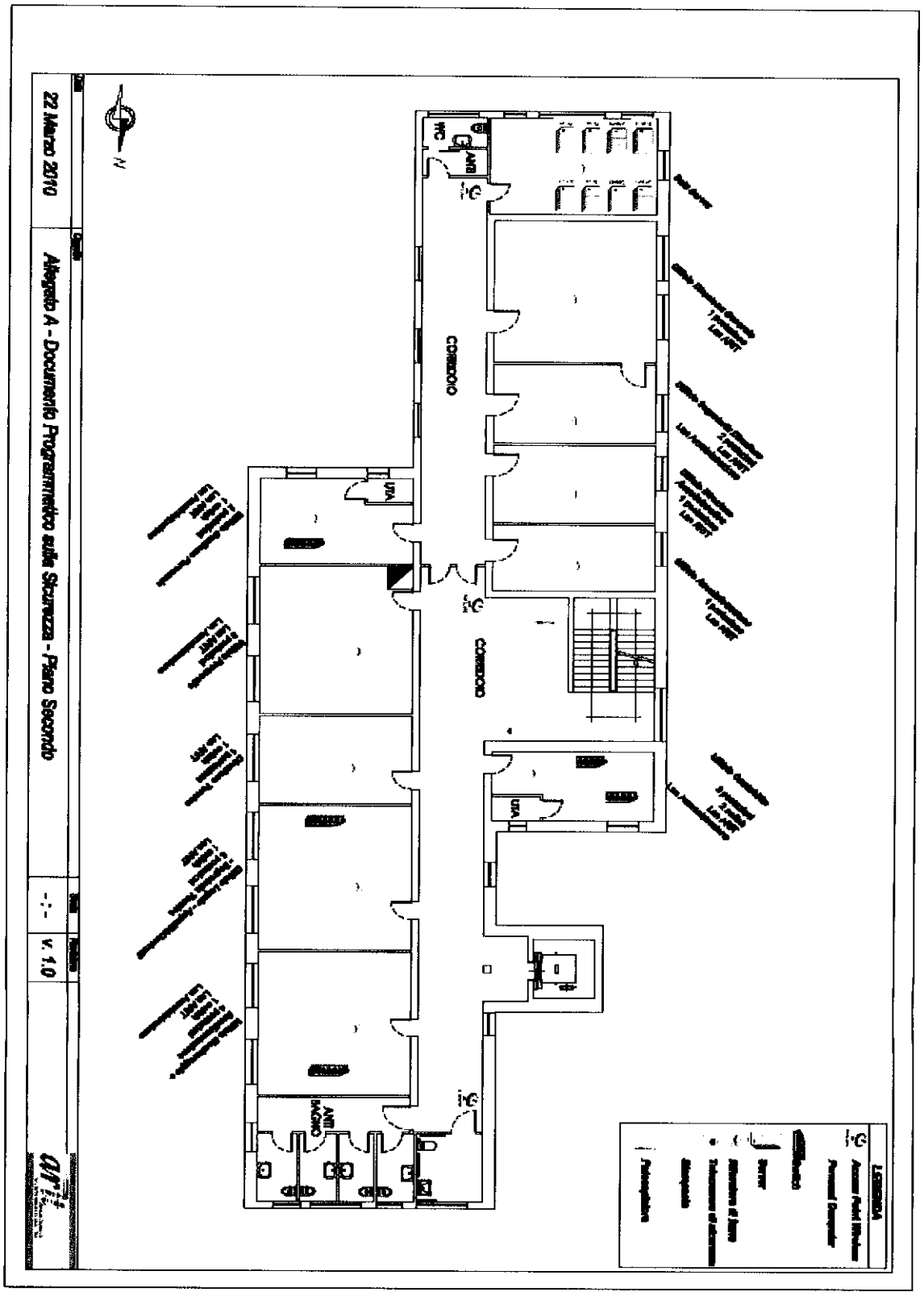
- ai principali concetti inerenti la materia di tutela dei dati personali (vedi All. L – Introduzione alla privacy)
- alle norme comportamentali per l'utilizzo delle attrezzature informatiche (vedi All. C – Norme d'uso delle attrezzature informatiche ARIT)

Il piano di programmazione degli interventi formativi ha previsto la partecipazione di tutti gli Incaricati Arit ad un corso sull'attuazione del decreto legge 196/2003 (tutela delle persone ed altri soggetti rispetto al trattamento dei dati personali). Tale corso è stato effettuato nelle date 14-15 Febbraio 2008 c/o la sede ARIT, sita in Tortoreto Lido, via Napoli 4.

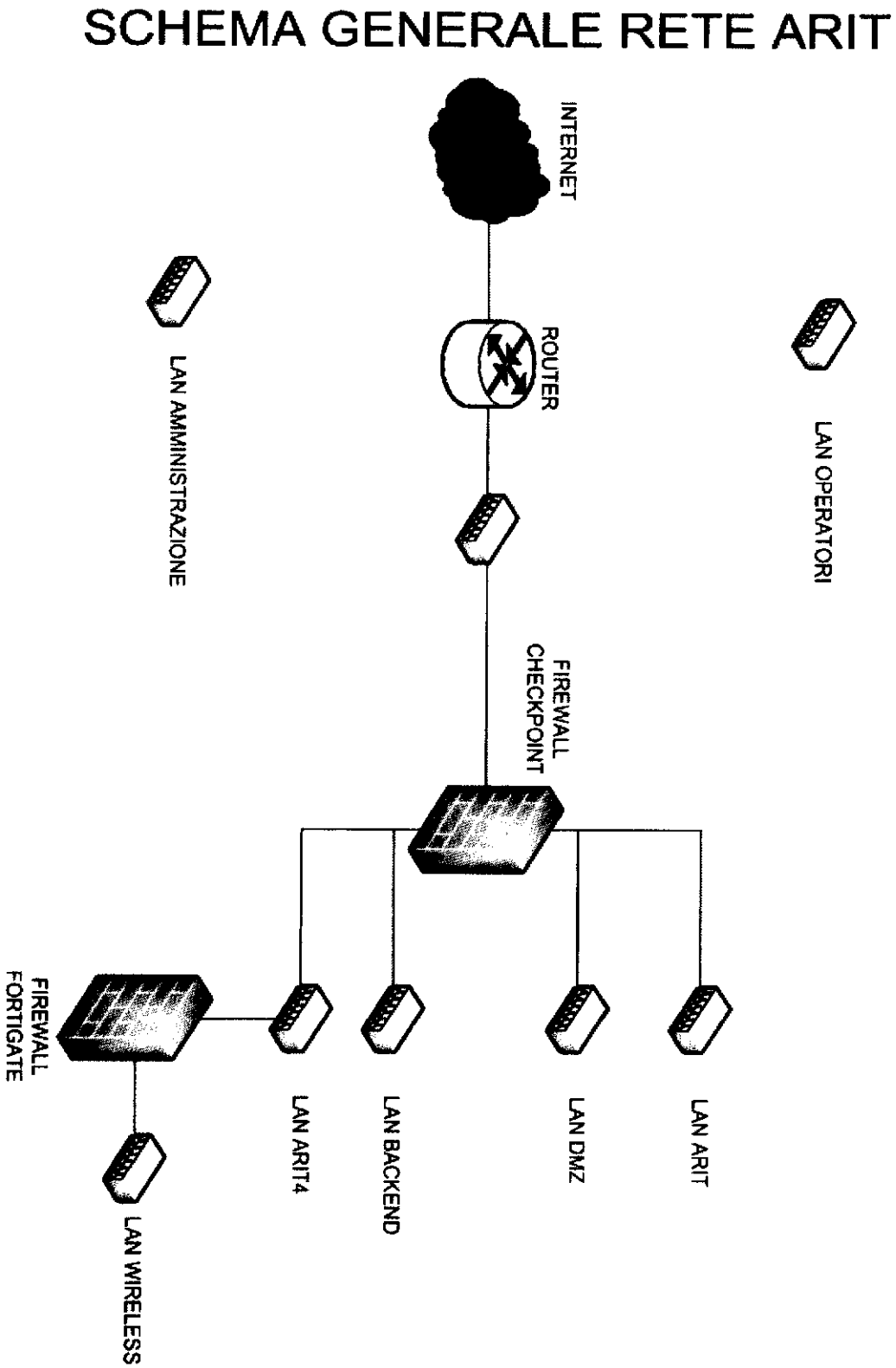
Allegato A – Piantina edificio

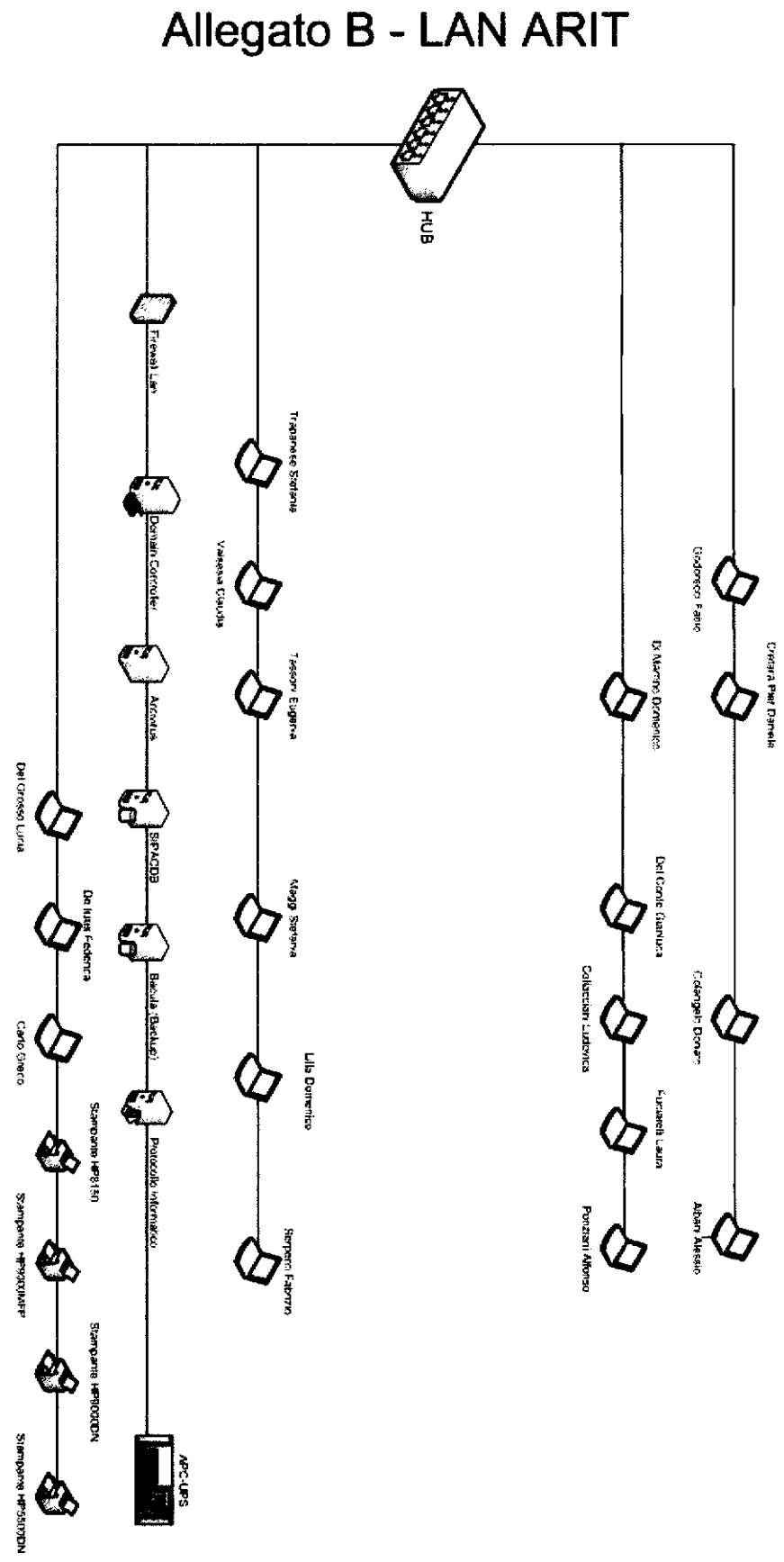



22 Marzo 2010
Allegato A - Documento Programmatico sulla Sicurezza - Piano Primo
-:-
v. 1.0
CORRIDOIO
LOCALE A DISPOSIZIONE
UTA
LEGENDA

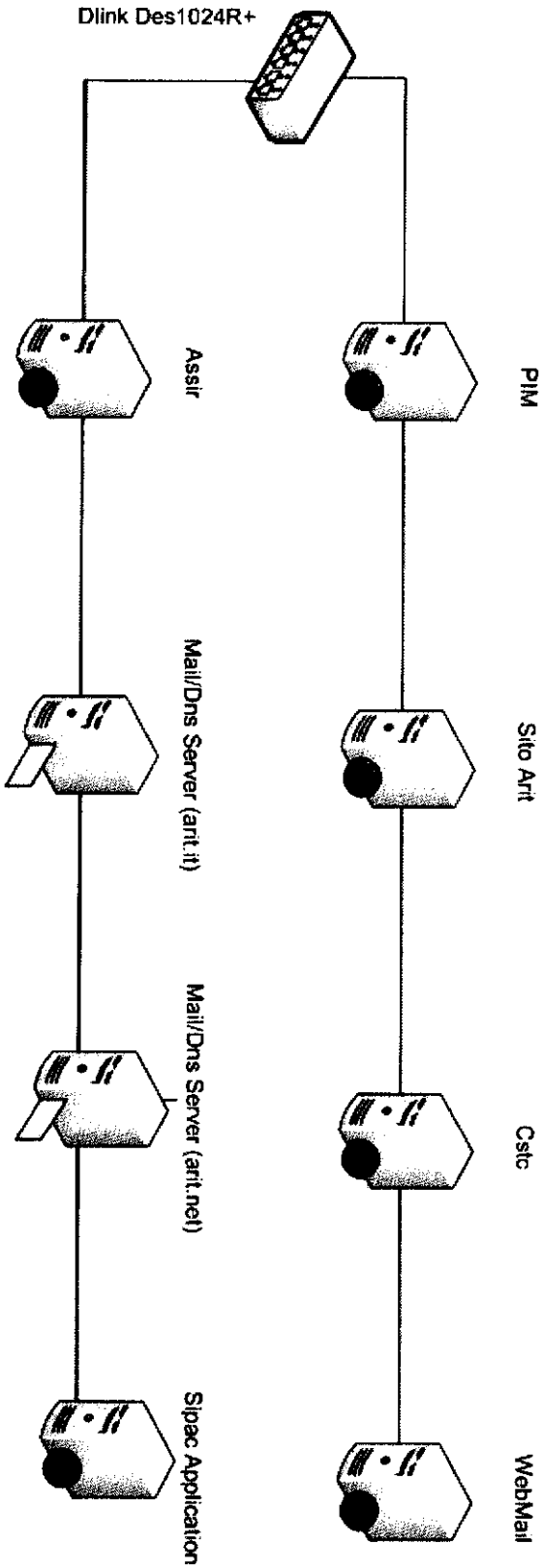

22 Marzo 2010
Allegato A - Documento Programmatico sulla Sicurezza - Piano Secondo
v. 1.0
N
CORRIDOIO
CORRIDOIO
WC
ANTI
UFFICIO
LEGENDA

Allegato B – Schema di rete

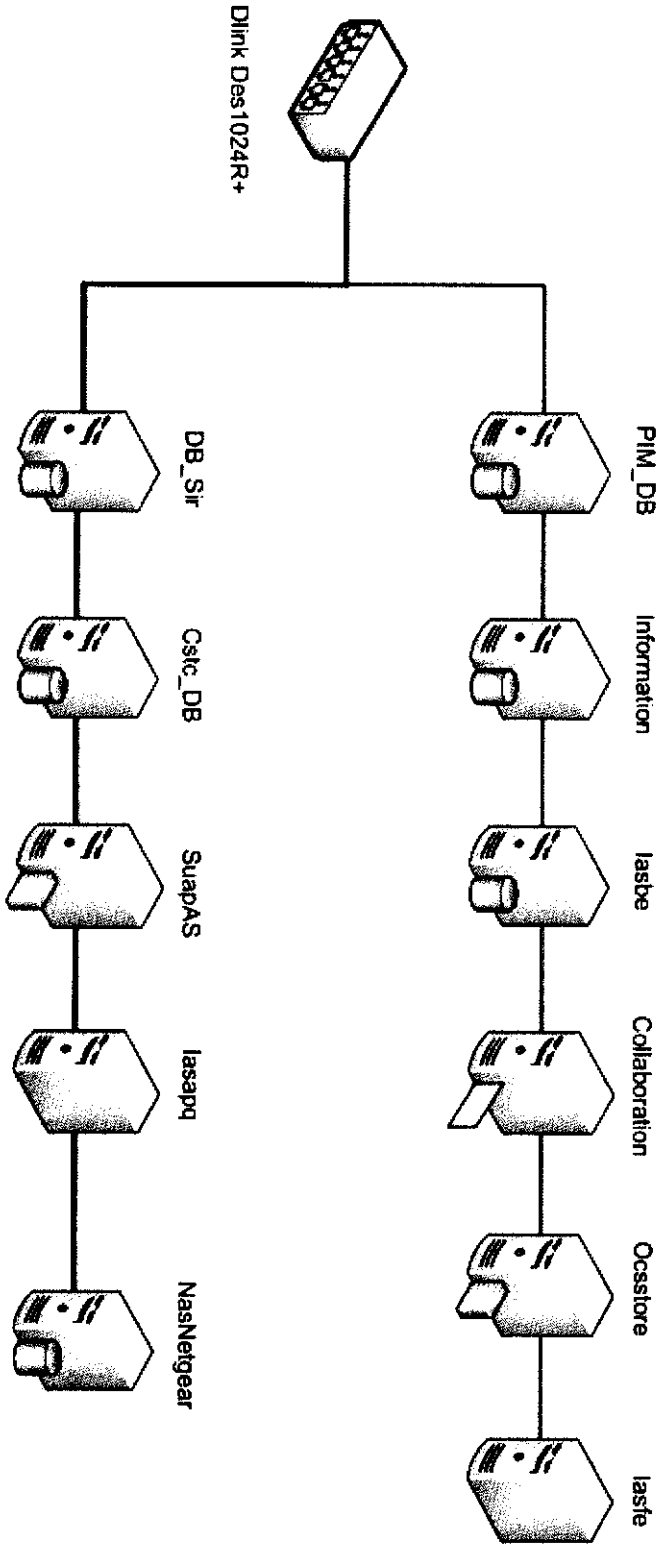



Allegato B - LAN ARIT
HUB
Firewall Lan
Domain Controller
Arconet
SIPACDB
Backup (Backup)
Protocollo Informatico
APC-UPS
Trapanese Stefania
Vanessa Claudia
Tessoni Eugenia
Magg Stefania
Lilli Domenico
Sampieri Fabrizio
Del Grosso Luna
Del Nista Federica
Carlo Grieco
Stampante HP8150
Stampante HP9000MFP
Stampante HP8100DN
Stampante HP5000DN
Giuliacci Fabio
Di Marino Domenico
Del Conte Gianluca
Colaiacomi Ludovica
Ponziani Alfonso
Cristina Pier Daniele
Cardarelli Donato
Lipparelli Laura
Albani Alessio

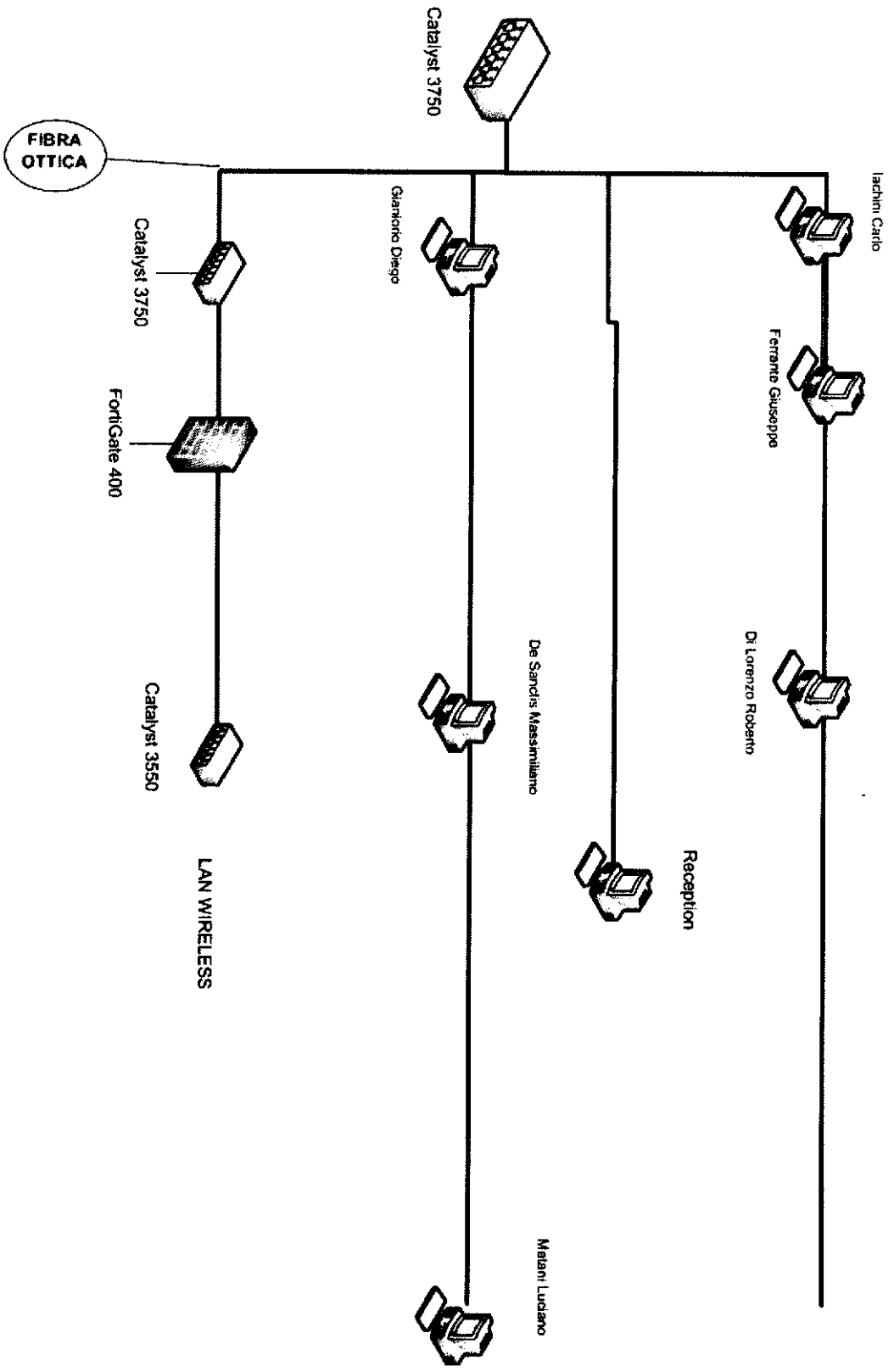
Allegato B – LAN DMZ



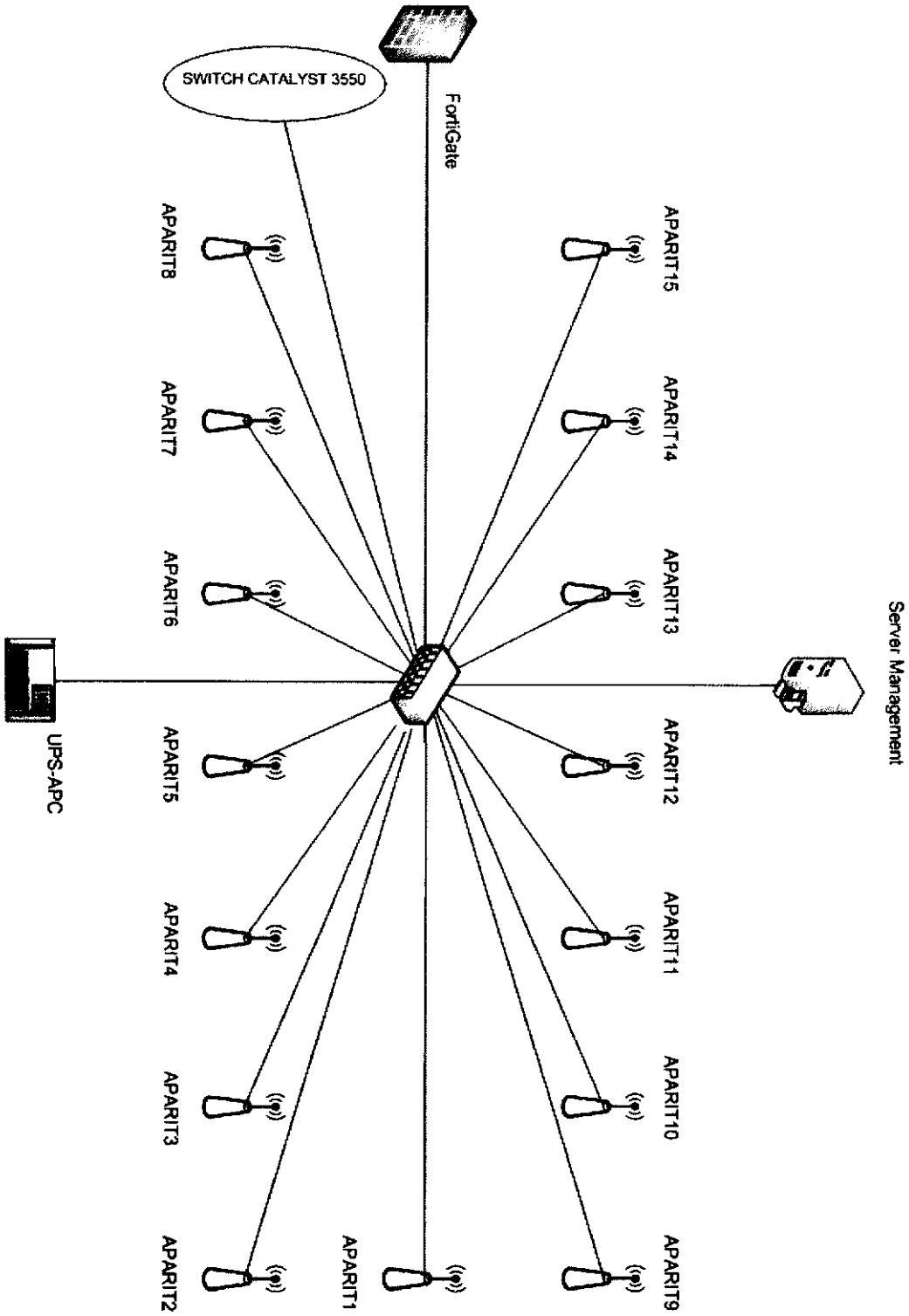
Allegato B - LAN BACKEND



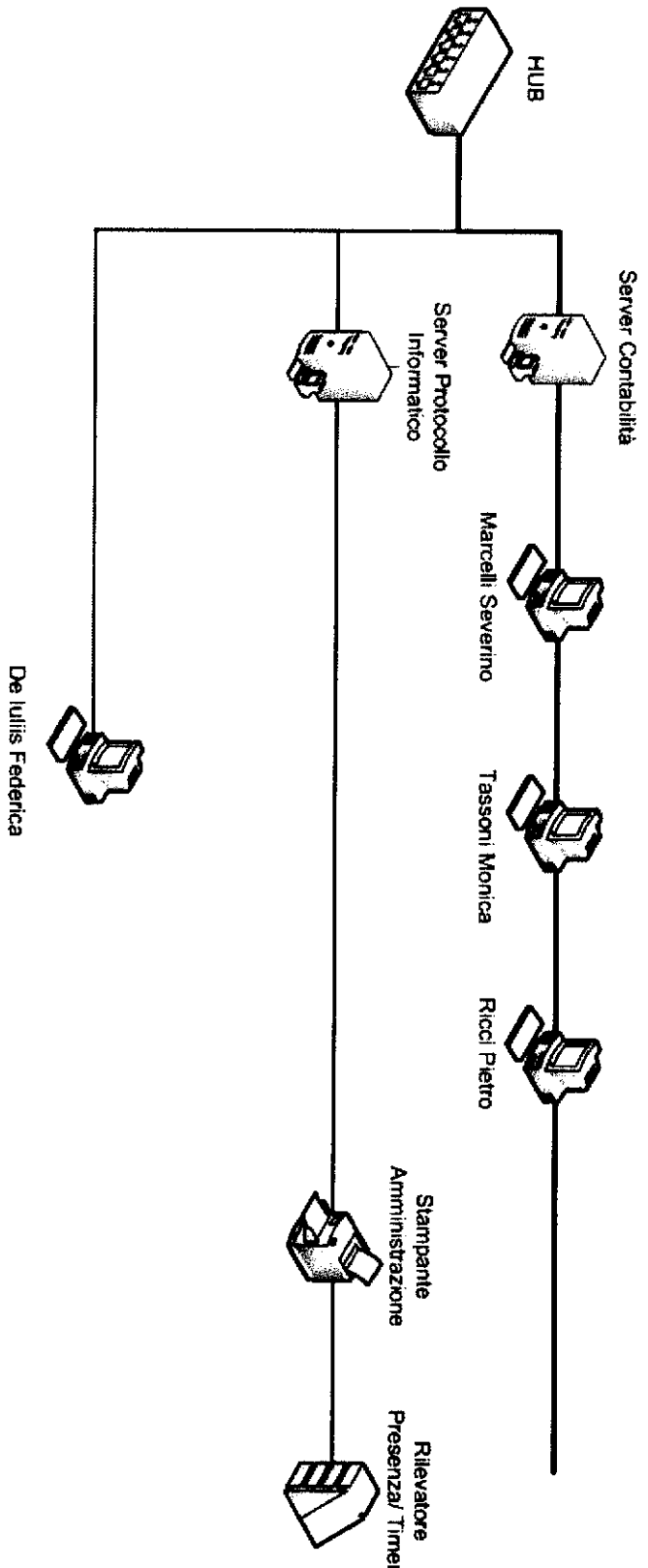
Allegato B - LAN ARIT4



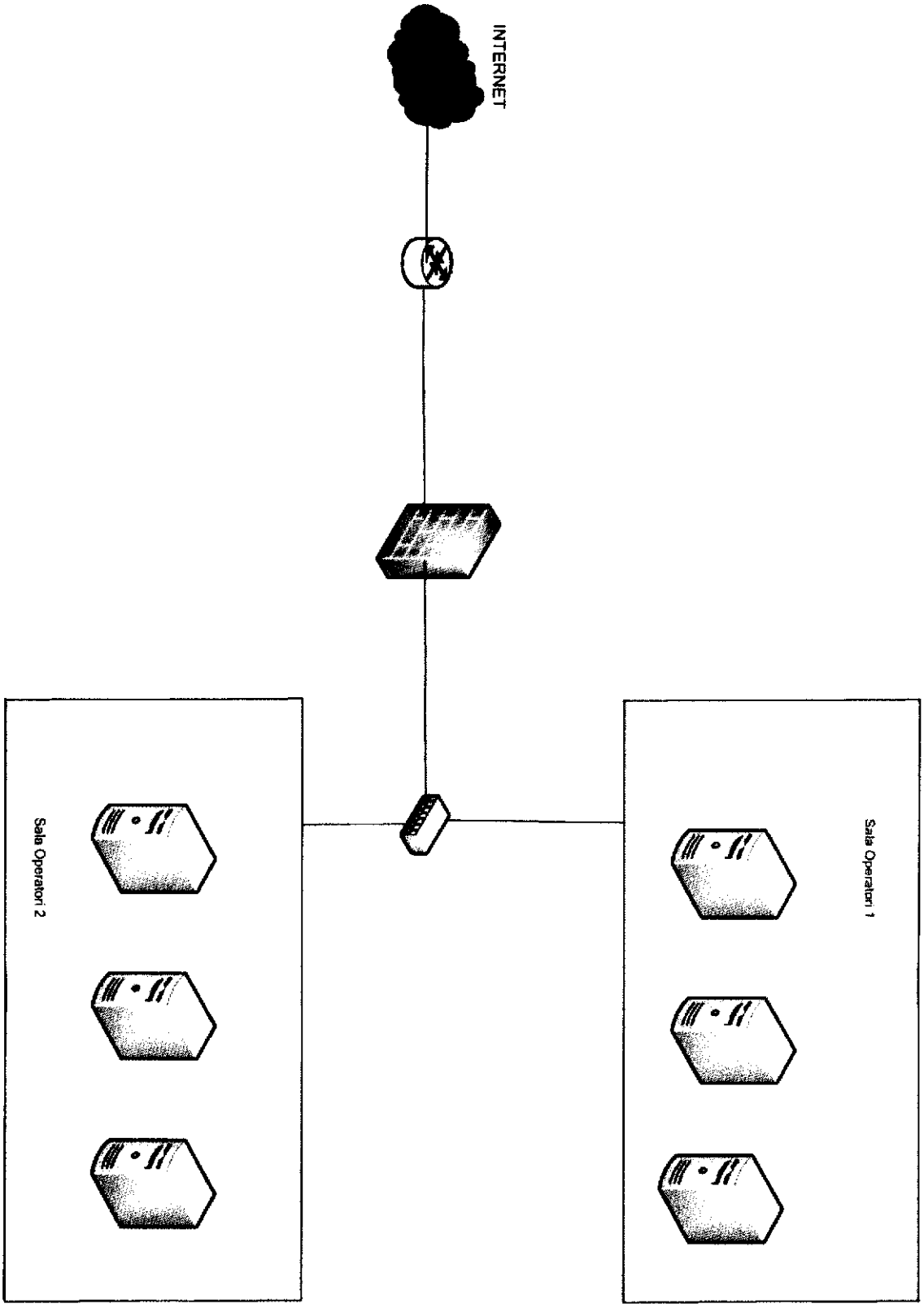
Allegato B - LAN WIRELESS



Allegato B - LAN AMMINISTRAZIONE



Allegato B - LAN OPERATORI



Allegato C – Norme d'uso delle attrezzature informatiche ARIT

Ai collaboratori/consulenti/dipendenti ARIT

Oggetto: norme d'uso per l'utilizzo delle risorse informatiche e telematiche ARIT

In riferimento all'utilizzo delle risorse informatiche e telematiche che l'ARIT mette a disposizione ai propri collaboratori/consulenti/dipendenti, si evidenzia che esso deve sempre basarsi su principi di diligenza e di correttezza.

Con la presente si elencano al fine di garantire:

- la massima efficienza delle risorse di calcolo
- la riservatezza e la sicurezza delle informazioni e dei dati
- l'omogeneità sulle modalità operative di utilizzo delle apparecchiature

una serie di norme, qui di seguito riportate, per responsabilizzare gli utenti nel corretto utilizzo delle succitate risorse.

1. Il Personal Computer (di seguito nominato PC) affidato all'utente è uno strumento di lavoro, pertanto ogni utilizzo non inerente allo svolgimento della propria attività lavorativa, può contribuire a porre in essere disservizi, costi di manutenzione e minacce alla sicurezza delle informazioni in esso contenute.

2. L'accesso al PC è protetto da una password che deve essere severamente custodita dall'utente. Inoltre tale password:
    a. va sostituita periodicamente almeno ogni 6 mesi (ogni 3 mesi in caso di trattamento di dati sensibili o giudiziari);
    b. deve essere composta da una sequenza di almeno 8 caratteri;
    c. non deve contenere riferimenti agevolmente riconducibili all'utente.
    d. Le password di amministrazione di tutti i sistemi informatici ARIT sono scritte e conservate all'interno di buste chiuse e siglate dal responsabile della password presso la cassaforte dell'Ufficio della Direzione Generale al secondo piano.

e. Le password di tutte le cartella e dei file eventualmente utilizzate sono scritte e conservate all'interno di buste chiuse e siglate dal responsabile della password presso la cassaforte dell'Ufficio della Direzione Generale al secondo piano.

3. E' consentito all'utente di modificare le configurazioni impostate sul proprio PC, solo previa autorizzazione dell'Area Tecnica.

4. Non è consentito agli utenti di installare autonomamente software di qualsiasi genere, poiché sussiste il pericolo di alterare la stabilità e la sicurezza del PC. In caso di necessità si deve contattare il personale dell'Area Tecnica.

5. Il PC deve essere spento ogni sera prima di lasciare gli uffici ed in caso di assenze prolungate.

6. Lasciare un PC incustodito può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'utilizzo indebito. Si raccomanda pertanto di bloccare l'accesso ogni qualvolta ci si allontani dal PC (per i sistemi Windows premere Bandierina + L) e di impostare lo screen saver in modalità "ripristino protetto da password".

7. Non è consentito l'uso sul proprio PC di nessun dispositivo di memorizzazione esterno (penne USB, dischi esterni, floppy, ...), salvo in casi di reale necessità che verranno comunque valutati dalla Direzione.

8. E' vietato collegare alla rete ARIT qualsiasi dispositivo senza averne avuto esplicita autorizzazione dal personale dell'Area Tecnica.

9. Ogni utente deve strutturare la cartella "Documenti" in "ARIT_NomeUtente" che deve essere costituita a sua volta dalle cartelle "Documenti_Definitivi" e "Documenti_Provvisori". Tutti la documentazione prodotta con qualsiasi strumento o sistema operativo, deve essere archiviata nelle cartelle suddette.
   Per gli utenti i cui computer sono connessi alla rete LAN AMMINISTRAZIONE valgono le stesse istruzioni sopra riportate ad eccezione per il fatto che per cartella Documenti si intende la cartella personale presente nel server Contabilità (configurata dal personale dell'Area Tecnica per ogni utente) a cui è possibile l'accesso tramite apposito Collegamento su Desktop. Qualora ci fossero incertezze relative all'essere connessi o meno alla LAN AMMINISTRAZIONE oppure alla possibilità di accedere alla propria Cartella personale si prega di voler contattare il personale dell'Area Tecnica.

10. E' cura dell'utente ritirare prontamente le stampe effettuate dai vassoi delle stampanti.

11. Le caselle di posta elettronica assegnate dall'Agenzia agli utenti, sono strumenti di lavoro; le persone titolari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

12. Al fine di minimizzare il fenomeno dello spamming è vietato utilizzare le caselle di posta elettronica:
    a. per la partecipazione a dibattiti in forum e/o mailing-list, salvo in casi di esplicita autorizzazione
    b. per la registrazione a siti i cui contenuti non siano legati all'attività lavorativa

13. E' buona norma evitare l'invio di messaggi completamente estranei allo svolgimento della propria attività lavorativa.

14. La rete Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa, è buona norma evitare la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

15. Si porta a conoscenza agli utenti che l'uso della rete Internet può esporre il sistema informativo dell'Agenzia a numerosi rischi tra cui:

    a. contagio da virus informatici
    b. installazione non autorizzata di software dannoso (spyware, malware, ...)
    c. accesso non autorizzato ai dati contenuti nei PC

    Pertanto l'ARIT ha posto in essere opportune misure di sicurezza per filtrare le connessioni verso indirizzi potenzialmente pericolosi, al fine di garantire l'integrità e la sicurezza del proprio sistema informativo.

16. Ogni qualvolta l'utente rileva una delle seguenti anomalie, si impegna a darne tempestiva comunicazione al personale dell'Area Tecnica

    a. Connessioni automatiche del browser alla rete internet
    b. Degrado delle prestazioni del PC
    c. Riavvio del sistema
    d. Blocco delle applicazioni in esecuzione

Tortoreto lì, 24 Novembre 2005

Il Direttore Generale

Allegato D – Gestione chiavi cassaforte 1° Piano

Al personale dell'Ufficio Reception

Oggetto: modalità operative di gestione delle chiavi della cassaforte 1° Piano

Con la presente si comunicano al personale della Reception le direttive in merito alle modalità di gestione delle chiavi della cassaforte situata al 1° piano presso l'ufficio denominato Area Tecnica 10

1) Le chiavi in oggetto possono essere consegnate solo ed esclusivamente al personale ARIT qui di seguito elencato:
   a. Sig. Donato Colangelo

   Ogni eccezione dovrà essere autorizzata formalmente dal Direttore Generale.
2) Ad ogni consegna il personale della Reception è tenuto ad annotare:
   a. Nome e cognome del consegnatario
   b. Data e ora di consegna
   c. Data e ora di restituzione
   d. Motivo
   e. Firma del consegnatario

Allegato E – Regole per l'accesso ai locali della sala server 1° Piano

1 - Personale autorizzato all'accesso ai locali della sala server 1° piano:

- Colangelo Donato
- Del Conte Gianluca

2 - Le chiavi per l'accesso ai locali della sala server 1° piano vengono prese in consegna (**dal personale autorizzato riportato al punto 1**) presso la portineria e vengono restituite presso la stessa nel momento in cui si è portato a termine l'intervento.

3 - Verranno istituiti due registri al fine di rendere possibile un controllo incrociato degli accessi presso i locali della sala server. Il primo registro, denominato "Registro A - Sala Server 1° Piano", sarà conservato presso la portineria mentre il secondo registro, denominato "Registro B - Sala Server 1° Piano", sarà disponibile nei locali della sala server.

4 - Il personale autorizzato si impegna a compilare entrambi i registri nei quali verranno riportati per ogni singolo accesso:
- data
- nome e cognome della persona che effettua l'accesso al locale
- orario di ingresso
- orario di uscita
- tipologia dell'intervento
- firma

5 - Qualora si presentasse la necessità di consentire l'accesso ai locali della sala server da parte di **personale non autorizzato** si procederà secondo le seguenti modalità:

5.1 - Nel caso in cui all'interno della struttura sia presente il personale autorizzato: la persona che ha la necessità di accedere ai locali verrà accompagnata da quest'ultimo, fermo restando l'obbligo della compilazione dei registri.

5.2 - Nel caso in cui all'interno della struttura il personale autorizzato sia assente: la persona che ha la necessità di accedere ai locali ne farà apposita richiesta al Direttore, fermo restando l'obbligo della compilazione dei registri.

In ogni caso sarà compito del personale della portineria assicurarsi che, la persona che effettua l'accesso al locale, compili il registro "Registro A - Sala Server 1° Piano" in ogni sua parte.

6 - Il personale della portineria sarà autorizzato all'accesso ai locali della sala server solo ed esclusivamente in assenza del personale autorizzato e solo ed esclusivamente per il controllo della temperatura che dovrà essere effettuato ad intervalli regolari di due ore. Anche il personale della portineria è tenuto alla compilazione dei registri. La temperatura del locale server è visualizzata sul display del condizionatore nell'angolo in alto a destra.
Poiché i locali della sala server ospitano macchine non in produzione non si rende necessario il controllo costante della temperatura del locale. Sarà cura del personale autorizzato avvisare la portineria della necessità di eseguire il controllo della temperatura.
Nei casi in cui si verifichi il blocco dell'impianto di condizionamento o la temperatura del locale sia superiore ai 24 gradi, il personale della portineria, facente parte della Vigilantes Group, provvederà ad informare la ditta responsabile della manutenzione.

7 - Nel caso in cui non sia possibile un intervento immediato da parte **della ditta responsabile della manutenzione**, si rende necessaria la procedura di spegnimento delle macchine sia per la loro salvaguardia, sia per diminuire la temperatura all'interno del locale.
Il personale della Vigilantes Group è a disposizione dell'Agenzia per effettuare tale intervento 24/7.

Allegato F – Regole per l'accesso ai locali della sala server 2° Piano

1 - Personale autorizzato all'accesso ai locali della sala server 2° piano:

- Colangelo Donato
- Del Conte Gianluca

2 - Le chiavi per l'accesso ai locali della sala server 2° piano vengono prese in consegna (**dal personale autorizzato riportato al punto 1**) presso la portineria e vengono restituite presso la stessa nel momento in cui si è portato a termine l'intervento.

3 - Verranno istituiti due registri al fine di rendere possibile un controllo incrociato degli accessi presso i locali della sala server. Il primo registro, denominato "Registro A - Sala Server 2° Piano", sarà conservato presso la portineria mentre il secondo registro, denominato "Registro B - Sala Server 2° Piano", sarà disponibile nei locali della sala server.

4 - Il personale autorizzato si impegna a compilare entrambi i registri nei quali verranno riportati per ogni singolo accesso:

- data
- nome e cognome della persona che effettua l'accesso al locale
- orario di ingresso
- orario di uscita
- tipologia dell'intervento
- firma

5 - Qualora si presentasse la necessità di consentire l'accesso ai locali della sala server da parte di **personale non autorizzato** si procederà secondo le seguenti modalità:

5.1 - Nel caso in cui all'interno della struttura sia presente il personale autorizzato, la persona che ha la necessità di accedere ai locali verrà accompagnata da quest'ultimo, fermo restando l'obbligo della compilazione dei registri.

5.2 - Nel caso in cui all'interno della struttura il personale autorizzato sia assente, la persona che ha la necessità di accedere ai locali ne farà apposita richiesta al Direttore, fermo restando l'obbligo della compilazione dei registri.

In ogni caso sarà compito del personale della portineria assicurarsi che, la persona che effettua l'accesso al locale, compili il registro "Registro A - Sala Server 2° Piano" in ogni sua parte.

6 - Il personale della portineria sarà autorizzato all'accesso ai locali della sala server solo ed esclusivamente in assenza del personale autorizzato e solo ed esclusivamente per il controllo della temperatura che dovrà essere effettuato ad intervalli regolari di un'ora. Anche il personale della portineria è tenuto alla compilazione dei registri.
Nei casi in cui si verifichi il blocco dell'impianto di condizionamento o la temperatura del locale sia superiore ai 24 gradi, il personale della portineria si impegna ad eseguire la manovra di ripristino dell'impianto di condizionamento documentata al punto 8. Qualora la suddetta manovra non sia sufficiente a ripristinare il funzionamento dell'impianto di condizionamento la portineria, facente parte della Vigilantes Group, provvederà ad informare la ditta responsabile della manutenzione.

7 - Nel caso in cui la manovra di ripristino dell'impianto di condizionamento non sia sufficiente a garantirne il corretto funzionamento e non sia possibile un intervento immediato da parte della ditta responsabile della manutenzione, si rende necessaria la procedura di spegnimento di alcune macchine sia per la loro salvaguardia, sia per diminuire la temperatura all'interno del locale.
Il personale della Vigilantes Group è a disposizione dell'Agenzia per effettuare tale intervento 24/7, secondo le modalità descritte al punto 9.

8 - La manovra di ripristino dell'impianto di condizionamento deve essere eseguita secondo le seguenti modalità:

- Portare la manopola rossa in posizione 0;
- Utilizzando il cacciavite situato sulla base superiore del condizionatore agire in senso orario sulle 2 viti a taglio situate nel pannello frontale del condizionatore;
- Aprire il pannello frontale;
- Premere il pulsante di colore azzurro situato in basso dietro il dispositivo etichettato SPH;
- Chiudere il pannello frontale e agire sulle appositi viti in senso antiorario;
- Portare la manopola rossa in posizione 1;
- Attendere che sul display venga visualizzato il simbolo "fiocco di neve".

9 - Segue la lista delle macchine di cui è necessario effettuare la procedura di shutdown in caso di temperatura elevata all'interno del locale.

- Firewall
- Antivirus
- Domain Controller
- Sito Arit

- Border Gate
- VCM
- Main Web 2
- Main Web 1
- Bacula
- Bacula Storage
- Mail Test
- Squid

Nel caso in cui in seguito allo spegnimento delle suddette macchine la temperatura resti comunque superiore ai 28 gradi si renderà necessario lo shutdown delle macchine rimanenti.

Allegato G – Modalità Accesso Uffici

Al personale dell'Ufficio Reception

Con la presente si comunicano al personale della Reception le direttive generali in merito alle modalità di gestione delle chiavi degli uffici ARIT.

- Le chiavi in oggetto possono essere consegnate solo ed esclusivamente al Personale Autorizzato ARIT. Di seguito viene fornito l'elenco dei nominativi relativo agli uffici.
  Ogni eccezione dovrà essere autorizzata formalmente dal Direttore Generale.
- Ad ogni consegna il personale della Reception è tenuto ad annotare:
  f. Nome e cognome del consegnatario
  g. Data e ora di consegna
  h. Data e ora di restituzione
  i. Firma del consegnatario

Ufficio	**Personale Autorizzato**
Ufficio Area Tecnica 1	Luciano Matani, Mauro Di Marco
Ufficio Area Tecnica 2	Laura Fuciarelli, Alfonso Ponziani,
Ufficio Area Tecnica 3	Fabio Goderecci, Massimiliano De Sanctis, Ludovica Collacciani, Pier Daniele Cretara, Roberto Di Lorenzo
Ufficio Area Tecnica 4	Del Conte Gianluca
Ufficio Area Tecnica 6	Domenico Di Martino, Alessio Albani
Ufficio Area Tecnica 7	Giuseppe Ferrante
Ufficio Area Tecnica 8	
Ufficio Area Tecnica 9	Donato Colangelo,
Ufficio Area Tecnica 10	
Ufficio Direzione Generale	Carlo Greco
Ufficio Segreteria Direzione	Federica De Iulis
Ufficio Direzione Amministrativa	Lucia Del Grosso
Ufficio Gestione Personale	
Ufficio Protocollo	Severino Marcelli,
Ufficio Direzione Tecnica	
Ufficio Contabilità	Pietro Ricci, Monica Tassoni
Ufficio Legale, Appalti&Contratti, Segreteria Tecnica	Stefania Trapanese, Claudia Valsesia, Eugenia Tassoni.
Ufficio Monitoraggio & Rendicontazione	Domenico Lilla, Stefania Maggi, Fabrizio Serpenti
Sala Server 1P	Donato Colangelo, Del Conte Gianluca
Sala Server 2P	Donato Colangelo, Del Conte Gianluca
Internet Data Center	Gianluca Del Conte, Donato Colangelo, Roberto Di Lorenzo, Giuseppe Ferrante, Domenico Di Martino

Allegato H – Norme Tecniche

Ai dipendenti/collaboratori tecnici ARIT

Oggetto: regolamento area tecnica per le modalità di impiego e configurazione delle attrezzature informatiche A.R.I.T.

Segue una lista di regole generali adottate dall'Area Tecnica per la configurazione delle attrezzature informatiche che l'ARIT mette a disposizione dei propri collaboratori, consulenti e dipendenti.

1 - Ogni personal computer (PC d'ora in poi) di proprietà dell'ARIT deve essere conforme ai seguenti requisiti minimi di configurazione:

- Account personale protetto con nome utente e password (di almeno 8 caratteri), configurato in maniera tale da non avere i privilegi di amministratore.
- La password assegnata è provvisoria ed è modificata dall'utente nel momento del primo accesso. E' prevista inoltre una scadenza semestrale della validità della password.
- Installazione di software Antivirus (configurato in maniera da eseguire l'aggiornamento in automatico) e software Firewall.

2 – Per tutti i PC che necessitano della connessione alla rete LAN ARIT, la configurazione della scheda di rete dovrà essere conforme al seguente schema:

- Indirizzo IP: 192.168.1.xyz;
- NetMask: 255.255.255.0;
- Default Gateway: 192.168.1.58 (firewall_lan);
- DNS: 217.220.87.179.

Verranno inoltre adottate le seguenti policy di sicurezza:

- Port Security: le porte di accesso alla rete LAN ARIT saranno configurate in maniera tale da poter effettuare un controllo di corrispondenza tra l'indirizzo MAC della scheda di rete del PC che viene connesso alla rete, e gli indirizzi MAC autorizzati sulla porta stessa. Salvo eccezioni dovute ad esigenze lavorative, per ogni porta, verrà configurato un singolo MAC in maniera tale da realizzare una corrispondenza 1 <-> 1 tra porte di accesso e PC.

3 – Tutti gli utenti che elaborano dati rilevanti per l'Agenzia hanno configurato un profilo nominale sul Controller di Dominio. Questa configurazione permette di eseguire il salvataggio automatico dei dati presenti nella cartella Documenti e nella cartella Desktop dell'utente.
I dati verranno salvati nel server che ospita il Controller di Dominio, rendendone così possibile il ripristino nei casi in cui si perdano.

I dati memorizzati nel Domain Controller vengono a loro volta salvati con cadenza giornaliera, in una unità di storage, che fornisce una soluzione di backup ridondato per i dati rilevanti.

4 - I PC che necessitano di accedere alla rete Internet verranno configurati secondo le seguenti modalità:

- Proxy Web (Indirizzo IP: 192.168.1.58 Porta: 3128). Questa configurazione presenta i seguenti vantaggi:
  - permette di sfruttare meccanismi di caching del traffico Internet limitando quindi il consumo di banda e garantendo prestazioni più elevate;
  - permette di filtrare le connessioni verso indirizzi non attinenti le attività dell'Agenzia (siti per adulti, siti warez, ...);
  - permette di implementare meccanismi di autenticazione per l'accesso ad Internet, tramite l'integrazione con il Domain Controller.
- Il firewall per l'accesso ad Internet (firewall_lan) verrà configurato in maniera tale da permettere solo ed esclusivamente l'utilizzo dei protocolli strettamente necessari (http, smtp, pop3, https, dns, imap);
- Dove è in uso il browser Internet Explorer, verrà configurato in maniera tale che le impostazioni relative alla privacy corrispondano al valore "Medio";
- Dove è in uso il browser Firefox, verrà configurato in maniera tale da accettare i cookie solo per il sito che li origina (blocco dei cookie di terze parti).

5 – I PC in uso presso gli uffici dell'amministrazione e la contabilità sono collegati tra loro attraverso una rete separata fisicamente dalla LAN ARIT denominata LAN AMMINISTRAZIONE. Per tali PC non è consentito l'uso della connessione ad Internet e della Posta Elettronica.

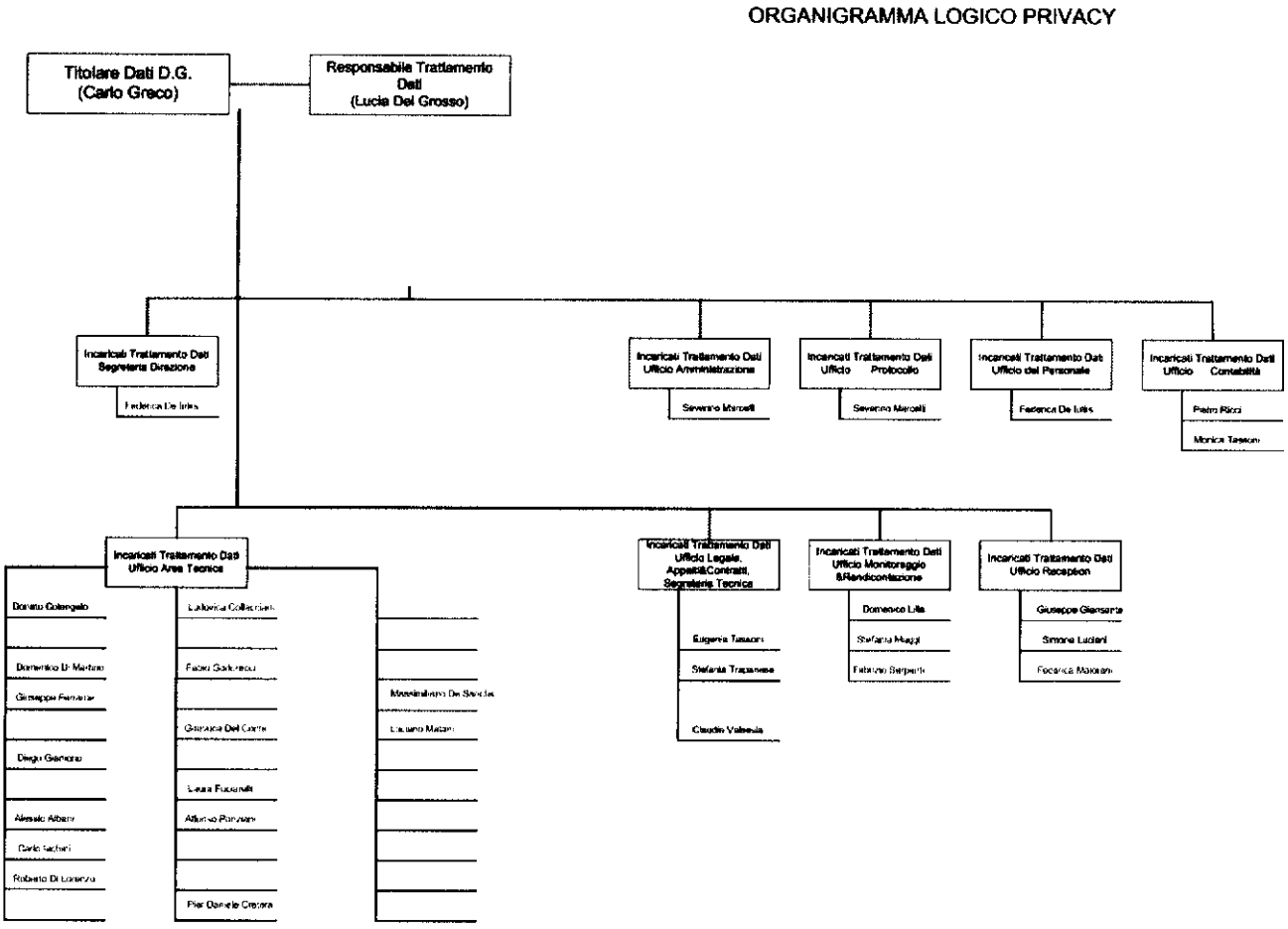
6 – L'uso di dispositivi di supporto rimovibili (Floppy, Cd Rom, Penne USB, Hard Disk esterni,...) è disponibile solo al personale autorizzato poiché la perdita o scomparsa di alcuni di essi può compromettere la riservatezza dei dati e/o l'integrità degli stessi.

7 – L'area tecnica si impegna nell'attività di costante aggiornamento del software installato sui PC valutando per ogni caso l'effettiva necessità e le conseguenze.

8 – L'area tecnica si impegna nell'attività costante di controllo/rimozione di software spyware accidentalmente installato nei PC.

9 – Nel caso in cui un dipendente/collaboratore/consulente cessi il rapporto di lavoro con l'Agenzia, l'area tecnica si impegna al blocco tempestivo di tutti i suoi accessi al sistema informativo.

Allegato I – Organigramma Logico Privacy



INTRODUZIONE ALLA PRIVACY (D.lgs. 196/2003)

Introduzione al Codice

Dal 1° Gennaio 2004 è entrato in vigore il D. Lgs. N° 196 del 30 Giugno 2003, denominato "Codice in materia di protezione dei dati personali", che sostituisce e integra tutta la precedente legislazione in materia (la più nota è la Legge *675/96*).
Introducendo nuovi principi di tutela e riservatezza dei dati, il Codice si pone come utile strumento per la protezione e salvaguardia degli stessi.
Oggetto di applicazione del Codice è quindi il **DATO PERSONALE.**

Legge 196/03: NORMATIVA

Le leggi sulla privacy in Italia

La prima legge italiana sulla protezione dei dati personali nasce nel 1996 (n° 675), nota come "legge sulla privacy", ha istituito la figura del garante per la privacy (autorità indipendente), per assicurare la tutela dei diritti, delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali.
La 675/96 stabiliva concetti fondamentali in merito al diritto di chiunque alla riservatezza ed alla tutela dei propri dati personali, e le "misure minime" di sicurezza necessarie per poter effettuare trattamenti di dati personali (Stabilite poi nel DPR 318/99).
Nel corso degli anni, il Garante ha emesso numerosi pronunciamenti tesi a chiarire o meglio specificare gli ambiti di applicazione.
Nel 2003 la vecchia 675/96 è stata sostituita dal nuovo "testo unico" approvato a Giugno che riorganizza la materia.

Il nuovo Testo Unico

Decreto legislativo 30 giugno 2003, n. 196: "Codice in materia di protezione dei dati personali" è entrato in vigore dal 01 Gennaio 2004 abrogando la precedente legge *675/96* accogliendo in sé tutti i pronunciamenti del Garante.

Il Codice della privacy garantisce che il *"trattamento dei dati personali"* si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La tutela si estende anche ai diritti delle persone giuridiche.

Le principali definizioni:

"Trattamento dei dati personali" è qualunque operazione o complesso di operazioni svolte con o senza strumenti elettronici, che concerne le operazioni di: raccolta dei dati, registrazione, organizzazione, conservazione, consultazione, elaborazione, blocco, modificazione, utilizzo, interconnessione, comunicazione, diffusione, cancellazione, distruzione, selezione, estrazione, raffronto.

"Dati personali" sono tutte le informazioni relative a persone fisiche o giuridiche, enti e associazioni, che consentano l'identificazione diretta o indiretta di questi stessi soggetti.
Ad esempio, sono dati personali rientranti nelle previsioni del Codice, oltre ai dati anagrafici ed economici, anche le immagini, i suoni e i codici identificativi riconducibili a un individuo.

I dati personali devono essere:

- **trattati in modo lecito e corretto;**
- **raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;**
- **esatti e, se necessario, aggiornati;**
- **pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;**
- **conservati in una forma che consenta l'identificazione dell'interessato, per un periodo di tempo non superiore a quello necessario agli scopi per cui sono stati raccolti o trattati.**

Esiste, inoltre, una categoria di dati i cosiddetti "dati sensibili" per i quali la legge prevede una tutela più forte rispetto agli altri.

"Dati sensibili" sono quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, politico, filosofico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I dati sensibili possono essere trattati soltanto con il consenso scritto dell'interessato e con l'autorizzazione del Garante.

"Dati giudiziari" sono quelli relativi a procedimenti penali ed a tutti i provvedimenti di cui all'art. 686, comma 1, lett. a) e d), nonché commi 2 e 3, del C.D.P. il cui trattamento è ammesso solo se autorizzato da espressa disposizione di legge o provvedimento del Garante, che ne specifichi le finalità, i tipi di dati e le operazioni autorizzate.

Per i soggetti pubblici il trattamento è consentito solo ed esclusivamente se è autorizzato da una legge, che specifichi quali sono i dati trattabili e le operazioni eseguibili, nonché le rilevanti finalità di interesse pubblico che si intendono perseguire. In tutti i casi, comunque, è necessario fornire all'interessato una completa informativa.

Ambito di applicazione

Secondo quanto indicato dall'art. 5 il codice viene applicato al trattamento dei dati personali effettuato da CHIUNQUE è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello stato.

Le figure interessate al trattamento

1. Il Titolare
2. Il Responsabile
3. L 'Incaricato
4. L 'interessato

Il titolare

Per **Titolare** si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza".
Anche con riferimento alle persone giuridiche, Titolare è a tutti gli effetti l'ente in quanto tale, e non già la persona fisica che ricopre una carica rappresentativa (amministratore, presidente etc.);
Il Titolare risponde, sotto ogni punto di vista, di eventuali trattamenti illeciti perpetrati al proprio interno, laddove non abbia adempiuto ai propri obblighi di definizione e corretta impostazione delle modalità da seguire per il trattamento dei dati e delle correlative misure di sicurezza.

Il responsabile

Per **Responsabile** si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati".

L'incaricato

Sono incaricati "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile"

L'Interessato

L'Interessato è la "persona fisica", la persona giuridica, l'Ente o l'Associazione cui si riferiscono i dati personali.

L 'informativa

Una corretta informativa è il presupposto iniziale della legittimità del trattamento dei dati.
A tal riguardo l'Art. 13 del Codice indica che la persona interessata al trattamento dei dati è informata per ISCRITTO o ORALMENTE circa:

1. le finalità e le modalità del trattamento cui sono destinati i dati;
2. la natura obbligatoria o facoltativa del conferimento dei dati;
3. le conseguenze di un eventuale rifiuto di rispondere;
4. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
5. i diritti di cui all'articolo 7 (diritto di accesso ai dati personali ed altri diritti);
6. gli estremi identificativi del titolare.

Il consenso

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.
Il consenso è validamente prestato solo se è espresso "liberamente" e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.
Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.
L'art. 24 del codice, "Casi nei quali può essere effettuato il trattamento senza il consenso" contiene un lungo elenco di casi riguardanti il trattamento dei dati senza consenso.
Il consenso non è richiesto, quando il trattamento:

- è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

- è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo.

Nella sostanza il trattamento può essere eseguito senza il consenso dell'interessato nei casi in cui sia "obbligatorio" (perché necessario per l'esistenza di un rapporto giuridico o perché previsto da una norma), oppure nei casi in cui si possa pregiudicare l'esercizio di altri diritti (di terzi o della collettività).

L'esclusione del consenso non fa venir meno l'obbligo di rendere l'informativa.