COMUNE DI CADONEGHE

REGOLE DI INSERIMENTO DELLE ANAGRAFICHE E DEGLI OGGETTI – ESTRATTO AURORA

Questo e' un estratto del Progetto Aurora che individua le modalità di inserimento delle anagrafiche e degli oggetti nelle operazioni di registratura (protocollo). Il progetto *Aurora* è stato promosso dalla Direzione generale per gli archivi del Ministero per i beni e le attività culturali, dall'Associazione nazionale archivistica italiana (ANAI) e dall'Università degli Studi di Padova

In alcuni casi le indicazioni che derivano dalla prassi in uso nel nostro Comune – evidenziate con * - sono state mantenute.

REGOLE GENERALI

PER PRASSI DEL COMUNE DI CADONEGHE E PER UNIFORMITA' DI INSERIMENTO CON LE ANAGRAFICHE IL PROTOCOLLO SI CONTINUA A INSERIRE **TUTTO MAIUSCOLO**

1 - Le abbreviazioni si utilizzano solo se approvate, le sigle non si puntano e l'acronimo si riporta anche sciolto

Le parole devono essere scritte complete e per esteso, senza storpiature, segni di punteggiatura o abbreviazioni nemmeno se di uso comune

Le abbreviazioni, le sigle e gli acronimi non vanno puntati. Infatti l'acronimo, di norma, viene inserito senza punti di separazione, in caratteri maiuscoli e si scrive di seguito alla denominazione per esteso della struttura a cui si riferisce, separato da un trattino preceduto e seguito da uno spazio

☺ ISTITUTO NAZIONALE DELLA PREVIDENZA SOCIALE - INPS
☹ *non* Istituto nazionale della previdenza sociale (INPS)

Anche quando una struttura viene comunemente individuata con una sigla o in forma abbreviata, la registrazione deve essere effettuata indicando sempre la denominazione per esteso, con l'aggiunta del relativo acronimo

☺ CASSA DI RISPARMIO DI GENOVA - CARIGE
☹ *non* CARIGE

Possono fare eccezione le sigle sindacali e le sigle dell'INPS, INAIL e CEMA quando sono riunite in un nuovo soggetto unificato. In tali casi può essere consentito riportare soltanto l'acronimo

2 - Aggettivi numerali ordinali e intervalli di numeri

I numeri si indicano utilizzando le cifre arabe. Il carattere a suffisso in apice degli aggettivi ordinali arabi è espresso al maschile con "o" in esponente [°] Anche i numeri ordinali si indicano in cifre arabe, accompagnati dalla "o" in esponente

☺ CELEBRAZIONI PER IL 55° ANNIVERSARIO…
☹ *non* Celebrazioni per il cinquantacinquesimo anniversario…

☺ DOTTORATO 19° CICLO
☹ *non* Dottorato XIX ciclo
☹ *non* Dottorato 19^ ciclo

I numeri romani si usano solo per numerare tomi, parti e capitoli di un libro, distinguere papi, sovrani e secoli e quando fanno parte di una denominazione di struttura

☺ PIO XII
☹ *non* Pio decimosecondo
☹ *non* Pio 12
☺ SECOLO XX
☹ *non* Secolo ventesimo

Per separare le centinaia dalle migliaia e le migliaia dai milioni si usa il punto; per separare i numeri interi dai decimali si usa la virgola.

La parola *euro* è indeclinabile (al plurale non si scrive *euri*). Essa va scritta per esteso, in lettere minuscole e dopo la cifra, evitando l'uso del suo simbolo [€].

Per l'indicazione di intervalli di numeri (pagine, date, numeri civici) si utilizza il trattino tra le due cifre che, in questo caso, non deve essere preceduto né seguito da spazi.

Per l'indicazione dell'anno scolastico o accademico si separano gli anni, indicati per esteso, con il trattino anche se sono tradizionalmente separati da una barretta , in quanto quest'ultima – soprattutto in fase di migrazione delle banche dati – potrebbe creare problemi al database.
aa 2008-2009

Un utilizzo frequente della barretta si trova nel linguaggio relativo al contenzioso, per separare le parti in causa. Anche in questo caso, è preferibile non utilizzare la barretta e trovare una parola. o una frase alternativa
☺ ROSSI MARIO CONTRO IL COMUNE DI LECCO
☺ ROSSI MARIO AVVERSO IL COMUNE DI LECCO
☹ *non* Rossi Mario / Comune di Lecco

3 - Nelle date si privilegia la leggibilità

All'interno dell'oggetto si privilegia l'immediata leggibilità di date e indicazioni numeriche Per questa ragione, le date si scrivono per esteso:
☺ CONVOCAZIONE PER IL 23 GIUGNO 2008
☹ *non* Convocazione per il 23/06/2008

RACCOMANDAZIONI PER L'INSERIMENTO DEL CORRISPONDENTE (MITTENTE –DESTINATARIO)

4 - Le intestazioni anagrafiche devono essere formate da elementi che identifichino il corrispondente in modo univoco

Gli elementi essenziali per l'identificazione univoca del corrispondente e la descrizione dell'anagrafica sono: il cognome e il nome per la persona fisica e la denominazione per la persona giuridica. Tuttavia, per ottenere un'informazione strutturata e per evitare le omonimie o le denominazioni simili, deve essere indicato anche un ulteriore elemento, quale l'indirizzo.

La "&" (*e* commerciale) riportata nella denominazione del corrispondente si scrive come semplice "e" nel campo di protocollo.

5 - Le descrizioni dei corrispondenti devono risultare il più possibile normalizzate

Le descrizioni dei corrispondenti devono risultare il più possibile normalizzate, allo scopo di facilitare la ricerca e di evitare la creazione di descrizioni in soprannumero (doppie e/o sbagliate). È indispensabile porre la massima attenzione al fine di non creare anagrafiche multiple relative allo stesso corrispondente.

*Nell'indicazione dei Comuni, Regioni, Province si deve evitare di inserire –di-

☺ COMUNE CADONEGHE
non Comune di Cadoneghe

- Nell'indicazione degli uffici pubblici indicare sempre il comune o la città

La registrazione anagrafica deve essere sempre riferita al corrispondente principale

Ulteriori precisazioni per ciascun corrispondente possono essere inserite in **note** (ad es, [*firmatario*], [*indirizzato a*] o [*all'attenzione di*]), in modo da evitare la registrazione di intestazioni doppie o multiple)

☺ COMUNE CAGLIARI [*firmatario*] BIANCHI LUCA - SINDACO
☺ COMUNE CAGLIARI [*firmatario*] ROSSI GIOVANNI - ASSESSOREAI LAVORI PUBBLICI
☹ *non* Comune di Cagliari - sindaco
☹ *non* Comune di Cagliari - Assessore ai lavori pubblici

☺ COMUNE ALESSANDRIA [*indirizzato a*] VERDI MATTEO - ASSESSORE ALLA CULTURA
☹ *non* All'assessore alla cultura del Comune di Alessandria

☺ UNIVERSITÀ DEGLI STUDI SALERNO [*firmatario*] VERDI GIOVANNI - DIRETTORE DEL DIPARTIMENTO DI STORIA
☹ *non* Direttore del dipartimento di storia
☹ *non* Verdi Giovanni, direttore del dipartimento di storia dell'Università degli Studi di Salerno

Le denominazioni dei corrispondenti si descrivono per esteso, senza preposizioni, abbreviazioni. o segni di punteggiatura

I nomi di persona e di struttura si scrivono completi e per esteso, senza storpiature segni di punteggiatura o abbreviazioni

☺ PREFETTURA Torino - UFFICIO TERRITORIALE DEL GOVERNO
☹ *non* Pref. di To.
☺ QUESTURA DI BARI
☹ *non* Questura BA

☺ MINISTERO DELL'ISTRUZIONE, DELLA UNIVERSITÀ E DELLA RICERCA - MIUR
☹ *non* Min. istr. Univ. e ricerca
☹ *non* M.I.U.R.
☹ *non* Mi.U.R.

☺ FONDAZIONE CASSA DI RISPARMIO DI PADOVA E ROVIGO - FONDAZIONE CARIPARO
☹ *non* Fondazione CR Padova Rovigo
☹ *non* Fondazione CARIPARO

☺ Zanni Rosiello Isabella
☹ *non* Z. Rosiello Isabella

6 - I nomi di persona fisica si indicano scrivendo prima il cognome e poi il nome, senza segni di separazione

Prevalendo in una banca dati l'ordine per cognome i nomi di persona fisica si indicano per esteso, scrivendo prima il cognome e poi il nome senza punteggiatura di separazione

☺ VERDI MATTEO
☹ *non* Matteo Verdi
☹ *non* Verdi M.
non Verdi, Matteo

Quando non è possibile distinguere il nome dal cognome nell'anagrafica della persona si riportano i nomi nella forma in cui sono indicati sul documento

☺ LUCA PAOLO (forma del nome e del cognome presenti sul documento)

Quando la persona scrive nella sua veste istituzionale o a nome della struttura a cui appartiene, l'anagrafica è formata solo dal nome della struttura. Nella registrazione, però, si descrive anche il nome della persona nel campo note [*firmatario*] o [*all'attenzione di*] seguito dalla qualifica. separata da un trattino

☺ COMUNE MILANO [*firmatario*] Bianchi Giovanni - Sindaco☹ *non* Comune di Milano Sindaco Giovanni Bianchi
☹ *non* Comune di Milano - Giovanni Bianchi Sindaco
☹ *non* Sindaco Giovanni Bianchi
☹ *non* Comune di Milano [*firmatario*] Sindaco Giovanni Bianchi

7 - I nomi di persona fisica si indicano senza titoli di deferenza o qualificazione del nome

I titoli accademici, di cortesia, di deferenza, di onorificenza, i predicati nobiliari, anche se il documento o la consuetudine li prevedono, non sono indicati nella descrizione dell'anagrafica.

In alcuni casi è possibile scrivere la qualità di professionista abbinata all'anagrafica di persona fisica, o il ruolo quando tale precisazione è funzionale alla migliore descrizione del corrispondente L'integrazione segue il nome di persona

☺ ROSSI MATTEO
☺ ROSSI MATTEO - INGEGNERE
☹ *non* dott. Avv. Rossi Matteo
☹ *non* ch.mo. prof Rossi Matteo
☹ *non* Matteo ing. Rossi
☹ *non* Preg.mo Matteo Rossi

☺ BIANCHI MARCO
☹ *non* Mons. Bianchi Marco
non Bianchi don Marco

8 - I nomi di struttura si descrivono con l'aggiunta del relativo acronimo delle virgolette e dei numeri eventualmente compresi

Quando il mittente è una struttura identificata nel documento o una forma abbreviata, di norma tramite sigla o acronimo l'operatore del sistema di protocollo descrive, se la conosce o è presente nel database, l'anagrafica della struttura in forma estesa, seguita dalla sigla o dall'acronimo.

L'acronimo si scrive in caratteri maiuscoli senza punti di separazione. Nel caso di sigle o acronimi composti da una parte stabile e da una parte variabile (ad es., su base regionale), è creata un'intestazione anagrafica per ogni forma

☺ CENTRO DI FORMAZIONE E STUDI PER IL MEZZOGIORNO - FORMEZ
😐 CENTRO DI FORMAZIONE E STUDI PER IL MEZZOGIORNO (forma accettata, ma sconsigliata)
☹ *non* Formez

☺ CENTRO STUDI INVESTIMENTI SOCIALI - CENSIS
☹ *non* Censis

☺ AZIENDA UNITÀ LOCALE SOCIO SANITARIA - AULSS 16 PADOVA
☹ *non* A.U.L.SS 16
☹ *non* A.U.L.S.S. n 16
☹ *non* A.U.S.L. 16

☺ ISTITUTO NAZIONALE DELLA PREVIDENZA SOCIALE - INPS - SEDE DI TORINO
☹ *non* I.N.P.S. Torino

☺ ISTITUTO NAZIONALE DI ASTROFISICA - INAF
☺ INAF (solo se non vi è alcun elemento per identificare la forma estesa)

☺ AGENZIA REGIONALE PROTEZIONE AMBIENTALE - ARPA
☺ AGENZIA REGIONALE PROTEZIONE AMBIENTALE TOSCANA - ARPAT

9 - L'anagrafica degli uffici e degli organi per l'ente o l'istituto di appartenenza è costituita dalla denominazione del contesto gerarchico di cui fanno parte, seguita da quella dell'articolazione funzionale

Per indicare un organo collegiale si precisa sempre prima l'ente o la struttura di appartenenza

Per l'amministrazione principale:

☺ UNIVERSITÀ DEGLI STUDI DI PAVIA - SENATO ACCADEMICO

☺ COMUNE LECCO - GIUNTA COMUNALE

Volendo scrivere a tutti i componenti di una commissione, non si registra mai il corrispondente privo dell'ente di appartenenza, anche se interno

Inoltre, si deve sempre evitare il "tutti" e il complemento di termine (ad es, "a", "al", "ai"), già implicito nella registrazione di un documento in partenza

☺ COMUNE SELVAZZANO DENTRO - COMMISSIONE EDILIZIA COMUNALE

☹ *non* Commissione edilizia comunale

☹ *non* Commissione edilizia comunale - Tutti i componenti

☹ *non* Ai componenti della Commissione edilizia

Quando una struttura. invia una circolare (o un documento assimilabile) a tutte le sue ripartizioni o a un gruppo omogeneo delle stesse o di altro genere, il mittente è identificato nella struttura stessa e il destinatario nelle ripartizioni nel loro complesso. Trattandosi di un atto interno indirizzato alla generalità delle ripartizioni della struttura, o a un gruppo identificato, non è necessario precisare le anagrafiche dei destinatari

☺ UNIVERSITÀ DEL SALENTO - DIPARTIMENTI

☹ *non* Ai Dipartimenti dell'Università del Salento

☺ LICEO SCIENTIFICO GIOBERTI DI MANTOVA - PERSONALE DOCENTE

non Al personale docente del Liceo scientifico Gioberti di Mantova

10 - Alle amministrazioni centrali dello Stato e alle regioni possono essere assegnate anagrafiche multiple; ai comuni e alle province di norma è assegnata una sola anagrafica con l'esclusione di anagrafiche con indirizzo PEC specifico

Per le amministrazioni centrali dello Stato, per le regioni e per le province e' consentito indicare, nell'intestazione anagrafica principale, le articolazioni gerarchiche interne fino al livello di riferimento

Nella compilazione dell'intestazione anagrafica degli uffici periferici dello Stato è omessa, di norma, l'indicazione dell'Amministrazione centrale

☺ SOPRINTENDENZA PER I BENI ARCHITETTONICI E PER IL PAESAGGIO PER LE PROVINCE DI BERGAMO COMO, LECCO, LODI, MILANO, PAVIA, SONDRIO, VARESE

☹ *non* Ministero per i beni e le attività culturali - Direzione regionale per i beni culturali e paesaggistici della Lombardia - Soprintendenza per i beni architettonici e per il paesaggio per le province di Bergamo, Como Lecco, Lodi, Milano, Pavia, Sondrio, Varese

☺ SOPRINTENDENZA ARCHIVISTICA PER IL LAZIO

☹ *non* Ministero per i beni e le attività culturali - MBAC - Soprintendenza archivistica per il Lazio

☺ QUESTURA DI BARI
☹ *non* Ministero dell'Interno - Polizia di Stato - Questura di Bari
non Polizia di Stato - Questura di Bari

Se una struttura dello Stato o di una regione ha un nome molto lungo o formato da numerose ripartizioni gerarchicamente articolate, è possibile ridurre l'intestazione anagrafica pur senza pregiudicarne la corretta identificazione, eventualmente omettendo i livelli gerarchici intermedi non indispensabili
☺ REGIONE TOSCANA - SETTORE INTEGRAZIONE SOCIO SANITARIA E NON AUTOSUFFICIENZA

Per i comuni e le province è indicata, di norma, una sola intestazione anagrafica senza alcuna distinzione in articolazioni statutarie o organizzative e indipendentemente dalle diverse sedi. Quando l'anagrafica corrisponde a un indirizzo PEC e' necessario inserire la denominazione e l'ufficio corrispondente all'indirizzo PEC

Anche se i comuni riportano sulla carta intestata l'indicazione di "città", in anagrafica si indica sempre "Comune "

☺ COMUNE RAGUSA
☹ *non* Città di Ragusa

Anche se le regioni e le province utilizzano carte intestate differenti (ad es, Regione, Consiglio regionale del Piemonte, Giunta provinciale, Consiglio provinciale), in anagrafica si privilegia sempre l'elemento "Regione" o "Provincia", con l'eventuale aggiunta di ulteriori indicazioni nel campo NOTE [*firmatario*] o nel campo [*all'attenzione di*]
☺ COMUNE NAPOLI [*FIRMATARIO*] ROSSI MARCO - CAPO RIPARTIZIONE URBANISTICA
☺ COMUNE NAPOLI - RIPARTIZIONE URBANISTICA (per l'amministrazione di appartenenza)
☹ *non* Rossi Marco, Capo ripartizione urb. del Comune di Napoli

11 - Se sono presenti più denominazioni relative alla medesima struttura, si descrive quella prevalente

Per i documenti di imprese (ditte individuali, società, cooperative, ecc) e di associazioni , che utilizzano modalità diverse per scrivere la loro denominazione o ragione sociale, si riporta il nome così come si presenta sulla carta intestata, sul timbro o su una dicitura sul documento stesso (descrizione che accompagna la sottoscrizione o l'intestazione "dattiloscritta")

La forma societaria (srl, spa, snc, etc) è scritta sempre con caratteri minuscoli, senza punti di separazione e viene indicata dopo il nome.
Quando il termine "società", "fondazione" o "associazione" è parte integrante del nome , tale indicazione non è separata dal nome stesso, ma vi rimane unita.
I nomi di studi (associati o di singoli, legali, pubblicitari, di commercialisti, ecc) sono riportati come per le ditte e associazioni, se chiaramente indicati sul documento, con l'esclusione dei titoli professionali, accademici e di deferenza.

Nel caso di un documento in cui sono indicate più sedi per lo stesso soggetto, e non è possibile identificare con certezza quella del mittente (considerando anche la localizzazione geografica eventualmente indicata a fianco della data), in anagrafica si descrive la sede legale o, in mancanza, quella presentata in maggiore evidenza oppure la prima in elenco

☺ ROSSI COSTRUZIONI SRL
☹ *non* Rossi costruzioni srl
☹ *non* ROSSI Costruzioni Srl

☺ MOTORS SAS
☹ *non* Motors sas

☺ ASSICURAZIONI GENERALI SPA
☹ *non* Assicurazioni Generali SpA

☺ SOCIETÀ DANTE ALIGHIERI
☹ *non* "Dante Alighieri" - Società letteraria

☺ STUDIO LEGALE BIANCHI GIOVANNI
☹ *non* Avv. Giovanni Bianchi
☹ *non* Studio avvocato G Bianchi
☹ *non* Avv Giovanni Bianchi studio legale

☺ STUDIO ASSOCIATO ARCHITETTI VERDI MARCO, BIANCHI MATTEO E ROSSI LUCA

12 - L'anagrafica di un documento che non comprende alcun elemento utile alla identificazione del mittente si descrive con la parola "Anonimo "

Quando un documento è privo di firma e non comprende alcun elemento utile all'identificazione del mittente l'anagrafica si compila con la parola "Anonimo"

13 - Le aggregazioni fra strutture si descrivono riportandone per esteso le denominazioni

RACCOMANDAZIONI PER LA REDAZIONE DELL'OGGETTO

Mentre il corrispondente si descrive, l'oggetto, richiede un lavoro di redazione. Esso, infatti è la sintesi dei contenuti di carattere giuridico, amministrativo e narrativo di un documento.

L'oggetto è il principale campo di ricerca strutturata e quindi deve essere registrato con coerenza e attenzione per garantire l'efficacia delle operazioni di recupero dell'informazione (*information retrieval*) Nell'equilibrio tra analisi e sintesi , il protocollista deve porsi la seguente domanda : «Quali parole possono essere significative per la ricerca del documento che si sta protocollando?»

13 - L'oggetto si redige ricercando un equilibrio tra analisi e sintesi

Per la redazione di un oggetto esaustivo è sufficiente indicare in modo chiaro, dal generale al particolare, l'azione e gli elementi principali del testo

☺ DECENNALE DEL PROGETTO TITULUS DEL 14 DICEMBRE 2007: AUTORIZZA LA MISSIONE A PADOVA
☹ *non* Aut miss PD 14/12/2007 int celeb decen Titulus
☹ *non* Autorizza missione
☹ *non* Autorizza la missione a Padova per la celebrazione del decimo anniversario di avvio del progetto Titulus 97, promosso dall'Università degli Studi di Padova, d'intesa con la Direzione generale per gli archivi, per la definizione di un titolario di classificazione per le Università italiane, realizzato dal Gruppo di lavoro appositamente costituito, del 14 dicembre 2007, ore 9-13, 14-18 Mezzo di trasporto proprio

☺ SI RILASCIA UNA ATTESTAZIONE A FINI PENSIONISTICI SUI SERVIZI PRESTATI ANTERIORMENTE ALLA NOMINA AI SENSI DELL'ART 145 DEL DPR 29 DICEMBRE 1973, N 1092
☹ *non* Dichiarazione ai sensi dell'art 145 del DPR 291273, n 1092

☺ COMUNICA I RISULTATI DELL'INDAGINE DI MERCATO PER L'ACQUISTO DI TELECOMANDI PROGRAMMABILI E RICEVITORI

Per la redazione dell'oggetto occorre identificare quindi l'azione principale a cui si riferisce il documento, tralasciando o ponendo in secondo piano eventuali altre azioni di rilevanza secondaria.

Nel caso in cui un documento contenga una sequenza numerica riferita a selezioni, gare , concorsi o altro, è significativo redigere l'oggetto riportando tutti i numeri di riferimento della sequenza. La rilevanza non è secondaria in quanto, oltre a individuare inequivocabilmente il procedimento a cui si riferisce, facilita la ricerca e offre maggiore sicurezza nella registrazione e nelle operazioni di recupero dell'informazione
☺ AVVISO DI INDIZIONE DELLE SELEZIONI PUBBLICHE NN 2008N60 - 2008N61 - 2008N62 - 2008N63 - 2008N64 - 2008N65
☹ *non* Avviso di indizione selezioni pubbliche dal n 2008N60 al n 2008N65

14 - L'oggetto si redige scegliendo forme verbali e lessici condivisi

15 - L'oggetto si descrive secondo i princìpi di univocità e uniformità

16 - L'oggetto si redige individuando le parole chiave che esprimono l'azione (o le azioni), facendo riferimento a una lista di termini utilizzabili

17 - La redazione dell'oggetto non si limita alla mera trascrizione dell'oggetto presente nel documento

Quando il protocollista effettua la registrazione deve, di norma, rielaborare l'oggetto alla luce del contenuto del documento

☺ SI COMUNICA CHE BIANCHI GIOVANNI È ASSEGNATO AL SETTORE AFFARI GENERALI DAL 1° GENNAIO 2009

☹ *non* Comunicazione assegnazione

☺ CONTROLLO ATTI - COMUNICA L'APPROVAZIONE DA PARTE DELLA GIUNTA REGIONALE DEL RENDICONTO GENERALE PER L'ANNO 2007

☹ *non* Controllo atti Comunicazione della decisione della Giunta regionale

☺ PROGRAMMA ALFA - SI TRASMETTE IL VERBALE RELATIVO ALL'ESTRAZIONE DEL CAMPIONE PER GLI ACCERTAMENTI DI AVVENUTA REALIZZAZIONE DEI LAVORI SUI PROGETTI CONCLUSI AL 31 DICEMBRE 2007

☹ *non* Programma Alfa - Trasmissione verbale

18 - L'oggetto di un documento si redige tenendo conto delle disposizioni vigenti in materia di protezione dei dati personali

I documenti possono contenere dati personali, compresi quelli sensibili e giudiziari. Essi possono riferirsi al mittente , al destinatario oppure ad altri soggetti interessati[1]

Nel redigere l'oggetto , pertanto, il protocollista dovrà tener conto anche dei princìpi generali contenuti nella normativa vigente in materia In altre parole – pur considerando che la registrazione dei documenti è prevista per legge e che, pertanto, le operazioni di trattamento di dati personali, effettuate nell'ambito di tale attività, perseguono uno scopo determinato e legittimo – è necessario che il protocollista rediga l'oggetto dei documenti contenenti dati personali, compresi quelli sensibili e giudiziari, non solo tenendo conto delle presenti raccomandazioni ma anche garantendo il rispetto dei principi di pertinenza e non eccedenza e di indispensabilità, previsti dal DLgs 196/2003[2].

In considerazione del fatto che le finalità perseguite attraverso la corretta redazione dell'oggetto sono quelle di garantire non solo la sua funzione giuridico-amministrativa, ma anche quella comunicativa facilitandone la ricerca, si evidenzia la necessità che il protocollista :

[1] DLgs 30 giugno 2003, n 196, *Codice in materia di protezione dei dati personali* (GU 29072003, n174) e successive modifiche e integrazioni, in particolare le definizioni contenute nell'art 4

[2] Con riferimento al principio di pertinenza e non eccedenza, applicabile a tutte le tipologie di dati personali, l'art 11, comma 1, lett d) del DLgs 196/2003, prevede che i dati personali oggetto di trattamento devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono trattati Inoltre, con riferimento al principio di indispensabilità, applicabile ai dati personali sensibili e giudiziari, si veda anche l'art 22, comma 3

- inserisca nell'oggetto gli eventuali dati personali identificativi del soggetto interessato solo nel caso in cui gli stessi siano pertinenti e non eccedenti rispetto alle finalità perseguite sopra ricordate Nei casi di particolare riservatezza è preferibile utilizzare solo le iniziali del nome e cognome oppure un codice identificativo;
- eviti accuratamente, in attuazione del principio di indispensabilità, di inserire nell'oggetto dati personali sensibili e giudiziari e, in particolare, quelli idonei a rivelare lo stato di salute e le abitudini sessuali dell'interessato

☺ DICHIARA LA CESSAZIONE DEL DIRITTO ALLE DETRAZIONI D'IMPOSTA PER FAMILIARI A DECORRERE DAL 1° GENNAIO 2009
☹ *non* Dichiarazione relativa alla cessazione del diritto alle detrazioni d'imposta per la figlia Giovanna Verdi, nata il 26 novembre 2007 a decorrere dal 1/1/09

☺ CHIEDE L'ASPETTATIVA VOLONTARIA DAL SERVIZIO A DECORRERE DAL 1° FEBBRAIO 2008
☹ *non* Richiesta di concessione aspettativa volontaria dal servizio per gravi motivi di salute a seguito dell'incidente automobilistico del 24/01/2008 a decorrere dal 01/02/2008

19 - L'oggetto non deve contenere riferimenti normativi muti o richiami non espliciti

I riferimenti normativi non costituiscono l'oggetto del documento , semmai ne formano il presupposto. Non è corretto, quindi, redigere l'oggetto di un documento limitandosi a citare un riferimento normativo senza ulteriori specificazioni Inoltre, un oggetto così formulato si rivela spesso inutile ai fini della successiva ricerca e rende di fatto impossibile ricavare indicazioni sull'effettivo contenuto giuridico del documento

☺ SI ACCOGLIE LA RICHIESTA DI TRASFERIMENTO DEL DIRITTO DI REIMPIANTO N 2898 DEL 17 NOVEMBRE 2007 PRESENTATA DALLA DITTA LA VIGNA
☹ *non* Regolamento (CEE) n 1493/1999, regolamento (CE) n 1227/2000 - Trasferimento diritto di reimpianto
☺ CHIEDE DI ESSERE ASSEGNATO ALLA STRUTTURA PERIFERICA DI NAPOLI
☹ *non* Istanza ex art 42-bis DLgs 151-2001

☺ COMUNICA IL MANCATO ACCERTAMENTO MEDICO LEGALE NEI CONFRONTI DEL DIPENDENTE BIANCHI GIOVANNI
☹ *non* Legge 6 agosto 2008, n 133

20 - Gli allegati non fanno parte del campo oggetto, ma si contano e si descrive la loro tipologia in campi separati

ALLEGATO N. 6

COMUNE DI CADONEGHE

FORMATI E DIMENSIONI
DEI DOCUMENTI INFORMATICI

I formati

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.
Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

Criteri di scelta dei formati

Ai fini della formazione, gestione e conservazione, è stato necessario indicare i formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

Le caratteristiche alle quali i formati rispondono sono le seguenti:

- **Apertura**: per apertura si intende la conformità a specifiche pubbliche. Perché sia aperto un formato deve essere ampiamente documentato e definito da chi lo produce e questa documentazione deve essere resa disponibile a chiunque voglia utilizzarlo. DigitPA consiglia fortemente di adottare solo formati approvati dall'ISO o ETSI.
- **Sicurezza:** s'intende la capacità del formato di essere immodificabile e immune dall'inserimento del codice malevolo.
- **Portabilità:** è la capacità di un formato di poter essere utilizzato ovunque o comunque sul maggior numero di piattaforme possibili. Un formato portabile non dipende dal sistema operativo o dall'hardware. I formati portabili sono, normalmente, quelli che hanno fatto uso per la loro implementazione di standard internazionali (si ritorna un po' sul concetto di apertura).
- **Funzionalità:** un formato funzionale deve poter essere utilizzato da (più) prodotti informatici che mettono a disposizione molte e diverse funzionalità l'uno dall'altro. Il formato dovrebbe dare sempre lo stesso risultato.
- **Supporto allo sviluppo**: fondamentalmente è il modo che l'organismo che gestisce il formato ha deciso per mantenere il formato stesso. Spesso ci si riferisce anche alle risorse messe a disposizione.
- **Diffusione:** è l'indice di utilizzo del formato. Quelli più usati, e quindi più diffusi, hanno una maggiore probabilità di "resistere" allo scorrere del tempo. Infatti un formato largamente diffuso oggi, sarà leggibile anche tra molti anni anche in caso di "soppressione" del formato per i nuovi documenti.

Ulteriori elementi da valutare sono stati l'efficienza in termini di occupazione di spazio fisico e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento.

Il documento si propone di fornire indicazioni sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico.

I riferimenti normativi sono individuati nel decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nel decreto legislativo 7 marzo 2005 n. 82, nel d.p.c.m 3/12/2013 "Regole tecniche sulla conservazione", nel d.p.c.m.3/12/2013 "Regole tecniche per il protocollo informatico" e nel d.p.c.m. 13/11/2014 "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici"

La regolamentazione si è resa necessaria al fine di gestire correttamente la documentazione informatica ricevuta e prodotta dal Comune, garantendone la leggibilità, autenticità ed efficacia probatoria nel tempo (conservazione/esibizione a norma), ma anche al fine di assicurare uniformità di comportamenti nei confronti dell'utenza esterna.

In base alle considerazioni espresse si individuano i seguenti formati come idonei alla produzione, gestione e conservazione dei documenti informatici gestiti dal Comune di Cadoneghe:

FORMATI	ESTENSIONI PRINCIPALI
PDF-PDF/A	.pdf, pdf/a
TIFF	.tif
JPG	.jpg, .jpeg
OFFICE OPEN XML (OOXML)	.docx,.xlsx, .pptx
ODF (OPEN DOCUMENTI FORMAT)	.ods, .odp, .odg, .odb
XML	.xml
TXT	.txt
EMAIL	.eml standard RFC 2822/MIME
P7M	.p7m

I formati audio e video non soddisfano i requisiti per poter essere conservati e non si ritiene siano da comprendere nei formati consentiti.

I formati ZIP, RAR e file cosiddetti "compressi", sono accettati se i documenti contenuti corrispondono ai formati consentiti.

La gestione di documenti informatici che non corrispondono ai formati consentiti sarà effettuata con la modalità previste per il documento cartaceo. Quindi i documenti saranno stampati, accompagnati dalla dichiarazione di conformità al documento digitale originale, protocollati e archiviati come un documento cartaceo.

LE DIMENSIONI DEI DOCUMENTI INFORMATICI

Il Comune di Cadoneghe riceve con la posta certificata documenti informatici con dimensioni fino a 30 MB.

Se i documenti informatici sono ricevuti a mezzo posta elettronica le dimensioni accettate sono fino a 12 MB.

apsystems®
progettazione e assistenza ICT

ALLEGATO N. 7

hyperSIC.*ProtocolloInformatico*

-

Manuale Utente
Procedure Operative

Aggiornato alla rel. 9.11

apSystems
progettazione e assistenza ICT

INDICE DEI CONTENUTI

INTRODUZIONE ALLA PROCEDURA 5

ACCESSO ALLA PROCEDURA 8

APPRENDERE LE OPERAZIONI FONDAMENTALI: IL PROTOCOLLO GENERALE 10

Protocollazione Documenti 10

Digitalizzazione Documenti 20

Archiviazione – Autenticazione 27

DOCUMENTI PROTOCOLLATI 28

Ricezione Posta 45

Spedizione Posta Esterna 47

Tabelle 50

REPERTORI 60

Inserimento 60

Consultazione 62

La Ricerca Documenti 63

Registri / Repertori 65

STAMPE 67

Stampe Selettive 67

CASELLA POSTALE 70

Posta in Arrivo 70

I comandi nella parte del Dettaglio e della griglia dei risultati: 73

Posta Inviata 77

Bozze 79

Gestione Sostituzioni 90

Gestione Fascicoli 90

Ricerche & Stampe 91

Tipi Archiviazione 92

GESTIONE WORKFLOW 94

Config. Procedimenti 94

Config. Processi 97

Operative 97

Statistiche Processi 101

Statistiche Caselle Postali 101

Visualizzazione Anomalie 102

Cancellazione Step 103

STAMPE 104

Registro di protocollo 104

Fascicoli 105

Ricerche & Stampe 107

UTILITÀ - TABELLE 108

Inizializzazione 108

Classificazioni 108

Gestione Corrispondenti 115

Documenti Base 118

Tipi Spedizione 118

Tipi Allegati 119

Registro Emergenza 120

Gestione supporti 121

Gestione Caselle Mail 122

Protoco_SYS 123

UTILITÀ - AVANZATE 1244

COMUNE DI CADONEGHE

METADATI

1 INTRODUZIONE

Il presente allegato illustra la struttura dei metadati relativi al documento informatico , al documento amministrativo informatico e al fascicolo informatico o aggregazione documentale informatica.

2 METADATI MINIMI DEL DOCUMENTO INFORMATICO

```
<?xmlversion="1.0"encoding="ISO-8859-1"?>
<xs:schemaxmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="documento">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="datachiusura" type="xs:date"/>
   <xs:element name="oggettodocumento" type="xs:string/>
   <xs:element name="soggettoproduttore">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="nome" type="xs:string"/>
      <xs:element name="cognome" type="xs:string"/>
      <xs:element name="codicefiscale" type="xs:string"/>
       </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="destinatario">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="nome" type="xs:string"/>
      <xs:elementname="cognome" type="xs:string"/>
      <xs:element name="codicefiscale"type="xs:string"/>
       </xs:sequence>
    </xs:complexType>
   </xs:element>
  </xs:sequence>
  <xs:attribute name="IDDocumento" type="xs:string"use="required"/>
 </xs:complexType>
</xs:element>
</xs:schema>
```

Informazione	Valori Ammessi	Tipo dato	xsd
Identificativo	Come da sistema di identificazione formalmente definito.	Alfanumerico20 caratteri	<xs:attribute name="IDDocumento" type="xs:string"use="required"/>
Definizione			
Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier(URI), il Digital Object Identifier(DOI) e l'International Standard Book Number(ISBN)			

Informazione	ValoriAmmessi	Tipodato	xsd
Data di chiusura	Data	Data formato gg/mm/aaaa	<xs:element name="datachiusura" type="xs:date"/>
Definizione			
Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile			

Informazione	ValoriAmmessi	Tipodato	xsd
Oggetto	Testo libero	Alfanumerico100 caratteri	<xs:elementname="oggettodocumento" type="xs:string/>
Definizione			
Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublic Core prevede l'analoga proprietà"Description"che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero delcontenuto			

Informazione	ValoriAmmessi	Tipodato	xsd
Soggetto produttore	nome:Testo libero	Alfanumerico40 caratteri	<xs:elementname="soggettoproduttore"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:elementname="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	cognome:testo libero	Alfanumerico40 caratteri	
	Codicefiscale: CodiceFiscale	Alfanumerico16 caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a produrre il documento informatico.			

Informazione	ValoriAmmessi	Tipodato	xsd
Destinatario	nome:Testo libero	Alfanumerico40 caratteri	<xs:elementname="destinatario"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	cognome:testo libero	Alfanumerico40 caratteri	
	Codicefiscale: CodiceFiscale	Alfanumerico16 caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico.			

```
<?xmlversion="1.0"encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="fascicolo">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="IPAtitolare" type="xs:stringmaxOccurs="1"/>
   <xs:element name="IPApartecipante" type="xs:string" minOccurs="0"maxOccurs="unbounded"/>
   <xs:element name="responsabile">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="nome" type="xs:string"/>
      <xs:element name="cognome" type="xs:string"/>
      <xs:element name="codicefiscale" type="xs:string"/>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:element name="oggettofascicolo" type="xs:string/>
     <xs:element name="documento" type="xs:string"maxOccurs="unbounded"/>
    </xs:sequence>
   <xs:attribute name="IDFascicolo" type="xs:string" use="required"/>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Informazione	ValoriAmmessi	Tipodato	xsd
Identificativo	Come da sistema di identificazione formalmente definito.	Alfanumerico20 caratteri	<xs:attribute name="IDFascicolo"type="xs:string" use="required"/>
Definizione			
Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e Permanente al fascicolo o aggregazione documentale informatica in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o Numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform ResourceIdentifier(URI), il Digital ObjectIdentifier(DOI)e l'International Standard Book Number(ISBN)			

Informazione	ValoriAmmessi	Tipodato	xsd
Amministrazione titolare	Vedi specifiche CodiceIPA	CodiceIPA	<xs:elementname="IPAtitolare"type="xs:string maxOccurs="1"/>
Definizione			
Amministrazione titolare del procedimento,che cura la costituzione e la gestione del fascicolo medesimo.			

Informazione	ValoriAmmessi	Tipodato	xsd
Amministrazioni partecipanti	Vedi specifiche Codice IPA	Codice IPA	<xs:elementname="IPApartecipante" type="xs:string"minOccurs="0" maxOccurs="unbounded"/>
Definizione			
Amministrazioni che partecipano all'iter del procedimento.			
Informazione	ValoriAmmessi	Tipodato	xsd
Responsabile	nome:Testo	Alfanumerico40	<xs:elementname="responsabile">

del procedimento	libero	caratteri	<xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	cognome:testo libero	Alfanumerico40 caratteri	
	Codicefiscale: CodiceFiscale	Alfanumerico16 caratteri	
Definizione			
Responsabile del procedimento			

Informazione	ValoriAmmessi	Tipodato	xsd
Oggetto	Testo libero	Alfanumerico100 caratteri	<xs:element name="oggettofascicolo" type="xs:string/>
Definizione			
Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublic Core prevede l'analoga proprietà"Description"che può includere ma non è limitata solo a: un riassunto analitico,un indice,un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.			

Informazione	ValoriAmmessi	Tipodato	xsd
Documento	Identificativodel documentocosì comedefinitodi alcapitolo3.	Alfanumerico20 caratteri	<xs:elementname="documento"type="xs:string" maxOccurs="unbounded"/>
Definizione			
Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità.			

PIANO DI SICUREZZA

Sommario

1 - OBIETTIVI DEL PIANO DI SICUREZZA 3
2 – GENERALITÀ 3
3 - FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA 4
4 - GESTIONE DEI DOCUMENTI INFORMATICI 5
4.1 - COMPONENTE ORGANIZZATIVA DELLA SICUREZZA 5
4.2 - COMPONENTE FISICA DELLA SICUREZZA 6
4.3 - COMPONENTE LOGICA DELLA SICUREZZA 6
4.4 - GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA 6
5 - TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI 7
5.1 - ALL'ESTERNO DELLA AOO (INTEROPERABILITÀ DEI SISTEMI DI PROTOCOLLO INFORMATICO) 7
5.2 - ALL'INTERNO DELLA AOO 7
6 - ACCESSO AI DOCUMENTI INFORMATICI 8
6.1 - UTENTI INTERNI ALLA AOO 8
6.2 - ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO 9
6.3 - UTENTI ESTERNI ALLA AOO - ALTRE AOO/AMMINISTRAZIONI 9
7 - CONSERVAZIONE DEI DOCUMENTI INFORMATICI 9
7.1 - SERVIZIO ARCHIVISTICO 9
7.2 - SERVIZIO DI CONSERVAZIONE SOSTITUTIVA 10
7.3 - CONSERVAZIONE DEI DOCUMENTI INFORMATICI E DELLE REGISTRAZIONI DI PROTOCOLLO 10
8 - POLITICHE DI SICUREZZA ADOTTATE DALLA AOO 11
8.1 - GENERALITÀ 11
8.2 - ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO 12
8.3 - PROFILI DI ACCESSO 12
8.4 - MODALITÀ DI CREAZIONE E GESTIONE DELLE UTENZE E DEI RELATIVI PROFILI DI ACCESSO 12
9.1 - POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATIVO 12
9.1.1 - Premessa 12
9.1.2 - Scopo 13
9.1.3 - Ambito di applicazione 13
9.1.4 - Politiche – Uso generale e proprietà 13
9.1.5 - Politiche - Sicurezza e proprietà dell'informazione 13
9.2 - POLITICHE - ANTIVIRUS 14
9.2.1 Premessa 14

9.2.2 Scopo 14
9.2.3 Ambito di applicazione 14
9.2.4 Politiche per le azioni preventive 14
9.2.5 Politiche per le azioni consuntive 16
9.3 - POLITICHE - USO NON ACCETTABILE 16
9.3.1 Attività di rete e di sistema 16
9.3.2 Attività di messaggistica e comunicazione 17
9.4 - LINEE TELEFONICHE COMMUTATE (ANALOGICHE E DIGITALI) 17
9.4.1 Scopo 17
9.4.2 Ambito di applicazione 17
9.4.3 Politiche – Scenari di impatto sull'Amministrazione 18
9.4.4 Politiche – Telefax 18
9.4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche 18
9.4.6 Politiche – Richiesta di linee telefoniche analogiche 18
9.5 - POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA 19
9.5.1 Scopo 19
9.5.2 Ambito di applicazione 19
9.5.3 Politiche 19
9.6 - POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA 19
9.6.1 Scopo 19
9.6.2 Ambito di applicazione 19
9.6.3 Politiche 19
9.7 - POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE 20
9.7.1 Scopo 20
9.7.2 Ambito di applicazione 20
9.7.3 Politiche – Usi proibiti 20
9.7.4 Politiche – Uso personale 20
9.8 - POLITICHE PER LE COMUNICAZIONI WIRELESS 20
9.8.1 Scopo 20
9.8.2 Ambito di applicazione 21
9.8.3 Politiche – Registrazione delle schede di accesso 21
9.8.4 Politiche – Approvazione delle tecnologie 21

Il presente allegato riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

1 - OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2 – GENERALITÀ

Il piano di sicurezza è stato redatto dal Responsabile dei Sistemi Informativi dell'Unione dei Comuni del Medio Brenta il quale si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, *di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali*, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.
Il Responsabile dei Sistemi Informativi ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza

giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;

- conservazione, a cura del Servizio Sistemi Informativi delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne e/o esterne qualificate;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- uso di codici identificativi (ad *es. separazione della parte anagrafica da quella "sensibile"*) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal titolare dei dati o suo delegato e, ove previsto dalle forze dell'ordine.

3 - FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano i formati indicati nell'allegato 6 del Manuale di gestione.
I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

4 - GESTIONE DEI DOCUMENTI INFORMATICI

Il sistema operativo del Sw di protocollo utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).
Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

4.1 - COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.
Nella conduzione del sistema informativo di gestione protocollo e della documentazione si utilizza un software gestionale web based nella seguente configurazione fisica:

- Server Applications (Server virtuale) dove sono installate le procedure di gestione del back office;
- Database Server (Server virtuale) dove è installato il DB della procedura;
- Server Applications (Server virtuale) dove è installato il portale verticale di gestione del front office.

L'infrastruttura virtuale è stata progettata su n. 3 nodi basata sulla piattaforma VMWare con l'obiettivo di aumentare l'efficienza e migliorare la funzionalità negli aspetti di Business Continuity e Disaster Recovery.

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- Responsabile Sistemi Informativi;
- Amministratore di sistema

4.2 - COMPONENTE FISICA DELLA SICUREZZA

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- La Server Room è situata al primo piano del Municipio del Comune di Cadoneghe ed è chiusa e accessibile solamente da personale autorizzato provvisto di chiave fisica;
- La Network Room è situata al piano terra del Municipio del Comune di Cadoneghe ed è chiusa e accessibile soamente da personale autorizzato provvisto di chiave fisica.

Esiste un sistema di allarme perimetrale dei locali che ospitano sia la Server Room che la Network Room collegata ad un istituto di vigilanza esterna.

4.3 - COMPONENTE LOGICA DELLA SICUREZZA

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del software di Protocollo, è stata realizzata attraverso:

- Assegnazione di credenziali agli utenti con profilazione che consideri l'Ufficio di appartenenza e le responsabilità assegnate allo stesso.

4.4 - GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul software di Protocollo che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall);
- dalle registrazioni del Software di Protocollo Informatico.

5 - TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale l'amministrazione oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

5.1 - ALL'ESTERNO DELLA AOO (INTEROPERABILITÀ DEI SISTEMI DI PROTOCOLLO INFORMATICO)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.
La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28

5.2 - ALL'INTERNO DELLA AOO

Gli Uffici dell'amministrazione si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica (eventualmente certificata ai sensi del decreto del Presidente della Repubblica n. 68 dell'11 febbraio 2005) in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l' "impiego della posta elettronica nelle pubbliche amministrazioni".

6 - ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso alla rete LAN di primo livello ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva di secondo livello.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.
Queste, in sintesi, sono le tipologie di gestione dei profili utenti:

La gestione Utenti: l'Amministratore di sistema dell'ente tramite hyperSIC.Amministratore può procedere alla creazione e gestione di tutti gli 'utenti' ossia tutti coloro che operano nel Sistema hyperSIC®, per avere l'accesso ai moduli applicativi.
La registrazione dell'utente avviene registrando i dati anagrafici, assegnando una LOGIN e una PASSWORD (temporanea), associando il profilo di utenza che può essere personalizzato per ciascuno in base a compiti e funzioni e indicando il/i Gruppi di lavoro a cui appartiene.

*La gestione Gruppi di Lavoro: o*gni operatore appartiene a un gruppo di lavoro con certi poteri di accesso. Il programma permette di garantire sistemi di sicurezza lasciando ampia libertà agli operatori competenti in materia, di creare o eliminare gruppi di lavoro associati ad una o più procedura con certi livelli di accesso. L'utente che lavora su una procedura può accedere anche alle altre se sono gestite dal suo stesso gruppo, mentre limitare l'accesso significa creare nuovi gruppi per singole procedure.

*La gestione Livelli d'accesso: u*na grande potenzialità del Sistema A. P. Systems è il perfetto controllo e la sicurezza negli accessi. Ogni operatore dell'Ente può lavorare con i poteri che l'amministratore di sistema conferisce lui partendo da una base, da un livello minimo già garantito gruppo per gruppo.

La gestione dei Log di connessione: fornisce lo strumento per l'analisi della sicurezza attraverso log di sistema e log segnalazioni e, in ottemperanza a quanto richiesto nel provvedimento sulla Protezione dei Dati Personali, permette l'esportazione di un file formato XML o XLS contenente tutti i log da masterizzare su un supporto non riscrivibile per la conservazione.

Il software di Protocollo adottato dall'amministrazione/AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del software di Protocollo può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

6.1 - UTENTI INTERNI ALLA AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal Responsabile di Protocollo dell'amministrazione/AOO. Tali livelli si

distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
La gestione delle utenze rispetta i seguenti criteri operativi:

- Profilo Protoco_Amministratore: assegnato all'Amministratore del sistema
- Profilo Protoco_SpedizioneMailPec: assegnato agli utenti non di protocollo generale che sono abilitati alla Spedizione di Pec
- Profilo Protoco_UfficioPG: assegnati agli utenti dell'Ufficio protocollo Generale
- Profilo Protoco_Utente: assegnato agli utenti di tutti gli altri uffici

6.2 - ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

- Profilazione utenti sul software di Protocollo

La visibilità completa sul registro di protocollo è consentita solo agli utenti appartenenti al Profilo Protoco_UfficioPG.
L'utente assegnatario dei documenti protocollati è invece abilitato con il profilo Protoco_Utente.
Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare,
la visibilità completa sul documento stesso è possibile solo agli utenti appartenenti al Profilo Protoco_UfficioPG.

6.3 - UTENTI ESTERNI ALLA AOO - ALTRE AOO/AMMINISTRAZIONI

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa.

7 - CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11 e D.P.C.M 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione ai sensi degli articoli20, commi 3 e 5bis, 23-ter, comma 4,43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

7.1 - SERVIZIO ARCHIVISTICO

Il responsabile del sistema archivistico dell'AOO ha individuato la sede dell'archivio dell'amministrazione. Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza).
Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.
Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.
Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.

Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti, (ovvero altri formati non proprietari di seguito indicati).

7.2 - SERVIZIO DI CONSERVAZIONE SOSTITUTIVA

Il responsabile della conservazione sostitutiva dei documenti fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida tracciate dal Responsabile di Protocollo, per una corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile.

Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni;
- assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
- definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento del contenuto dei supporti.

7.3 - CONSERVAZIONE DEI DOCUMENTI INFORMATICI E DELLE REGISTRAZIONI DI PROTOCOLLO

I luoghi di conservazione previsti per i supporti contenenti le registrazioni di protocollo e le registrazioni di sicurezza sono differenziati in base al livello di sicurezza loro attribuito.
È compito dell'ufficio che si occupa del servizio di sicurezza del sistema informativo l'espletamento delle seguenti procedure atte ad assicurare la corretta archiviazione, la disponibilità e la leggibilità dei supporti stessi.
L'archiviazione di ogni supporto viene registrata in un specifico file di cui è disponibile la consultazione per le seguenti informazioni:

- descrizione del contenuto;
- responsabile della conservazione;
- lista delle persone autorizzate all'accesso ai supporti, con l'indicazione dei compiti previsti;
- indicazione dell'ubicazione di eventuali copie di sicurezza;
- motivi e durata dell'archiviazione.

È stato implementato e viene mantenuto aggiornato un archivio dei prodotti software (nelle eventuali diverse versioni) necessari alla lettura dei supporti conservati.
Presso il sistema informativo sono altresì mantenuti i sistemi con la configurazione hardware necessaria al corretto funzionamento del software.
Nell'archivio di cui al terzo capoverso del presente paragrafo, viene quindi indicato anche:

- il formato del supporto rimovibile;
- il prodotto software col quale è stato generato e la versione della *release*;
- la configurazione hardware e software necessaria per il suo riuso.

Deve essere inoltre indicata l'eventuale necessità di *refresh* periodico dei supporti.

Il personale addetto alla sicurezza del sistema informativo verifica la corretta funzionalità del sistema e dei programmi in gestione e l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento sostitutivo del contenuto su altri supporti.

8 - POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.
Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'AOO intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.
È compito del Responsabile di Protocollo assistito dal Responsabile dei sistemi Informativi procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal CNIPA o a seguito dei risultati delle attività di *audit*.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

8.1 - GENERALITÀ

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.
Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).
Gli utenti del servizio di protocollo, in base agli Uffici di appartenenza, ovvero in base alle rispettive competenze hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.
Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente:
  - pubblica che permette l'identificazione dell'utente da parte del sistema (*userID*);
  - privata o riservata di autenticazione (*password*);
- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione sono assegnati agli utenti dal Responsabile di Protocollo che si avvale di un utente così detto privilegiato (amministratore). Gli utenti del servizio di protocollo una volta identificati sono suddivisi in n. 4 profili d'accesso, sulla base delle rispettive competenze.
Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli Uffici e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO sono costantemente aggiornate a cura del Responsabile di protocollo.

8.2 - ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO

Gli utenti abilitati accedono al software di protocollo attraverso un browser internet alla seguente Url: http://hypersic.cadoneghenet.it/hypersic/protocollo

Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.

Il "file delle password" utilizzato dal servizio di accesso è una struttura crittografata e accessibile soltanto da un processo di sistema.

Le sessioni multiple con la stessa *user ID* sono proibite e impedite dal software di Protocollo.

8.3 - PROFILI DI ACCESSO

- Profilo Protoco_Amministratore: assegnato all'Amministratore del sistema
- Profilo Protoco_SpedizioneMailPec: assegnato agli utenti non di protocollo generale che sono abilitati alla Spedizione di Pec
- Profilo Protoco_UfficioPG: assegnati agli utenti dell'Ufficio protocollo Generale
- Profilo Protoco_Utente: assegnato agli utenti di tutti gli altri uffici

8.4 - MODALITÀ DI CREAZIONE E GESTIONE DELLE UTENZE E DEI RELATIVI PROFILI DI ACCESSO

Al fine di procedere alla creazione delle utenze viene comunicato dal Responsabile di Servizio con apposito modulo al Responsabile di Protocollo gli utenti da abilitare ed i relativi privilegi.

In caso di smarrimento della password l'utente richiede la rigenerazione al Responsabile dei Sistemi informativi.

9.1 - POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATIVO

9.1.1 - Premessa

1. L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

2. Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

9.1.2 - Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.
2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
3. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

9.1.3 - Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati della ditta AP Systems Srl includendo tutto il personale affiliato con terze parti.
2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

9.1.4 - Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
3. Le singole aree o settori sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.
4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
5. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

9.1.5 - Politiche - Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni sei mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
3. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in *stand-by* con un comando specifico.

4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
8. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.
9. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

9.2 - POLITICHE - ANTIVIRUS

9.2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.
I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.
I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

9.2.2 Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

9.2.3 Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

9.2.4 Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.

- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
- Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
- Non utilizzare i server di rete come stazioni di lavoro.
- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.

- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico... [omissis]...che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il Responsabile di Protocollo in accordo con il Responsabile Sistemi Informativi

stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

9.2.5 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

9.3 - POLITICHE - USO NON ACCETTABILE

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
3. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

9.3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.

9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
   a) accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
   b) attività di "sniffing";
   c) disturbo della trasmissione;
   d) spoofing dei pacchetti;
   e) negazione del servizio;
   f) le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
   g) attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

9.3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.
1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

9.4 - LINEE TELEFONICHE COMMUTATE (ANALOGICHE E DIGITALI)

9.4.1 Scopo

1. Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).
2. Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

9.4.2 Ambito di applicazione

1. Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

9.4.3 Politiche – Scenari di impatto sull'Amministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
2. Il *primo* è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.
3. Il *secondo* scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

9.4.4 Politiche – Telefax

1. Dovrebbero essere adottate le seguenti regole:
   - le linee fax dovrebbero essere approvate solo per uso istituzionale;
   - nessuna linea dei telefax dovrebbe essere usata per uso personale;
2. Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.
3. Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

9.4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.
2. Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

9.4.6 Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;
- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato

9.5 - POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

9.5.1 Scopo

1. Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

9.5.2 Ambito di applicazione

1. Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

9.5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
2. Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

9.6 - POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA

9.6.1 Scopo

1. Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.

9.6.2 Ambito di applicazione

1. Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

9.6.3 Politiche

1. Il personale dell'Amministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. Tale accesso dovrebbe essere rigidamente controllato usando sistemi di autenticazione forte, quali: password da usare una sola volta (one time password), sistemi di firma digitale o tecniche di sfida/risposta (challenger/response).
2. È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive.
3. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.

4. Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

9.7 - POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

9.7.1 Scopo

1. Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

9.7.2 Ambito di applicazione

1. La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

9.7.3 Politiche – Usi proibiti

1. Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

9.7.4 Politiche – Uso personale

1. È considerato accettabile l'uso personale della posta istituzionale dell'Amministrazione a condizione che:
   - i messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
   - venga utilizzata una ragionevole quantità di risorse pubbliche;
   - non si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.
2. Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
3. L'Amministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli "usi proibiti" di cui sopra.

9.8 - POLITICHE PER LE COMUNICAZIONI WIRELESS

9.8.1 Scopo

1. Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
2. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

9.8.2 Ambito di applicazione

1. La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.
2. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

9.8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

9.8.4 Politiche – Approvazione delle tecnologie

1. Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.