Ministero dell'Istruzione, dell'Università e della Ricerca

IC VILLONGO

Allegati al

Manuale di Gestione

Del Protocollo Informatico

-

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Sono escluse dalla protocollazione, ai sensi dell'art. 53. c. 5 del DPR n. 445/2000 le seguenti tipologie documentarie:

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)
- convocazioni ad incontri o riunioni e corsi di formazione interni
- delibere, disposizioni interne, ordini di servizio e comunicazioni al personale
- modulistica attinente a ferie, missioni, fornitura di materiali ed equipaggiamenti informatici, rapporti valutativi e documentazione simile
- atti notificati a mano ai dipendenti
- ricevute di ritorno delle raccomandate A.R

REGOLE DI RACCOLTA E CONSEGNA DELLA CORRISPONDENZA CONVENZIONALE AL SERVIZIO POSTALE NAZIONALE

1. La corrispondenza viene quotidianamente consegnata dall'incaricato dell'Ufficio Postale a mezzo cassetta postale allocata all'esterno della scuola;
2. La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, viene consegnata in busta chiusa al servizio postale pubblico entro la mattinata ;
3. Gli Uffici Utente devono far pervenire la posta in partenza all'Ufficio Posta della UOP generale che esegue la spedizione, entro e non oltre le ore 12.00 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto all'interno dell'Amministrazione/AOO un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.
Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto

16.17.1 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE PER TUTTE LE AMMINISTRAZIONI

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241, dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

PIANO DI ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

Il seguente elenco di registri di protocollo diversi dal registro di protocollo informatico è il risultato di un censimento preliminare dei diversi registri di protocollo in uso presso l'amministrazione.

MASSIMARIO DI SCARTO

TIPOLOGIA	CONSERVAZIONE
ACCERTAMENTO CERTIFICAZIONE DI QUALITA'	∞
ACCERTAMENTO SANITARIO	∞
ACCERTAMENTO TECNICO PER MALATTIE PROF.LI	∞
ACCORDO DI RETE CON SCUOLE O ENTI	∞
ACQUISTO IMMOBILE	∞
ALBO DEL PERSONALE	∞
ALLEGATO DOCUMENTO VALUTAZIONE RISCHI	∞
ANNUARIO SCOLASTICO	∞
ASSEGNAZIONE SEDE	∞
ATTESTATO PARTECIPAZIONE CORSO FORMAZIONE E AGGIORNAMENTO	∞
ATTO ACCORPAMENTO SCUOLE	∞
ATTO COSTITUTIVO COOP. ALUNNI	∞
ATTO DI SCARTO DOCUMENTI	∞
ATTO ELEZIONE OO.CC.	∞
AUTORIZZAZIONE COLLABORAZIONE PLURIMA	∞
AUTORIZZAZIONE DI SICUREZZA LOCALI	∞
AUTORIZZAZIONE ESERCIZIO LIBERA PROFESSIONE	∞
AUTORIZZAZIONE LEZIONI PRIVATE	∞
BANDO BORSA DI STUDIO	∞
BANDO PER STAGE	∞
BILANCIO ANNUALE	∞
BORSA DI STUDIO	∞
CARTA DEI SERVIZI	∞
CATOLOGO BIBLIOTECA	∞
CERTIFICATO DI RESIDENZA	∞
CERTIFICATO DI SANA E ROBUSTA COSTITUZIONE	∞
CERTIFICATO DI SERVIZIO DEL PERSONALE	∞
CERTIFICATO DI STUDIO	∞
CERTIFICATO NASCITA	∞
CERTIFICAZIONE DI QUALITA'	∞
CERTIFICAZIONE DI SICUREZZA IMPIANTI	∞
CIRCOLARE INTERNA	∞
CONTO CONSUNTIVO	∞
CONTRATTO ASSUNZIONE PERSONALE	∞
CONTRATTO COSTRUZIONE	∞
CONTRATTO DI COSTRUZIONE	∞
CONTRATTO ESPLETAMENTO DI SERVIZI	∞
CONTRATTO FORNITURA MATERIALE	∞
CONTRATTO INDIVIDUALE	∞
CONTRATTO PER FORNITURA DI MATERIALE	∞
CONTRATTO PRESTAZIONE DI VARIA NATURA	∞
CONTRATTO RISTRUTT. MANUTENZIONE	∞
CONVENZIONE DI CASSA CASSIERE ISTITUTO	∞
CORRISPONDENZA ARRIVO	∞
CORRISPONDENZA RELATIVA A COOP. ALUNNI	∞
CORRISPONDENZA USCITA	∞
DECRETO ASPETTATIVA	∞
DECRETO DELEGATO	∞
DECRETO DI ASSENZA	∞
DECRETO DI NOMINA	∞
DECRETO DI TRASFERIMENTO	∞

DECRETO PER CONGEDO MATERNITA' ANTICIPATA	∞
DECRETO PER CONGEDO PARENTALE	∞
DECRETO PER CONGEDO STRAORDINARIO	∞
DELIBERA COMITATO SCOLASTICO	∞
DETERMINA DEL DIRIGENTE	∞
DIPLOMA	∞
DISEGNO IMMOBILE DI PROPRIETA'	∞
DISEGNO TECNICO IMPIANTI O ATTREZZATURE	∞
DISOGNO IMMOBILE IN USO	∞
DISPENSA AGGIORNAMENTO PERSONALE	∞
DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA INVALSI	∞
DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA OCSE	∞
DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA RAV	∞
DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA SIDI	∞
DOC RELATIVO A PROGETTO OCSEA	∞
DOC. ACQUISITA PER CONCILIAZIONE	∞
DOC. AGGIORNAMENTO PERSONALE	∞
DOC. AMBITI DISCLIPINARI OO.CC	∞
DOC. ASSISTENZA SCOLASTICA	∞
DOC. AZIONE LEGALE DIPENDENTE	∞
DOC. COMODATO IMMOBILE	∞
DOC. CONGEDO PARENTALE	∞
DOC. CONGEDO PER ASPETTATIVA	∞
DOC. CONGEDO PER MATERNITA'	∞
DOC. CONGEDO PER MATERNITA' ANTICIPATA	∞
DOC. CONGEDO STRAORDINARIO	∞
DOC. CONSULENZA COLLABORAZIONE ENTE LOCALE	∞
DOC. CONSULENZA ESPERTO ESTERNO	∞
DOC. CONSULENZA ISTITUZIONI ENTI VARI	∞
DOC. DELIBERATIVO A COOP. ALUNNI	∞
DOC. DIRITTO ALLO STUDIO	∞
DOC. GRUPPO DI LAVORO OO.CC	∞
DOC. INSERIMENTO ALUNNI STRANIERI	∞
DOC. INTITOLAZIONE SCUOLA	∞
DOC. ISTRUTTORIO COMITATO SCOLASTICO	∞
DOC. ISTRUTTORIO COMMISSIONE OO.CC	∞
DOC. ISTRUTTORIO PER COOP. ALUNNI	∞
DOC. POSIZIONE PREVIDENZIALE	∞
DOC. POSIZIONE STIPENDIALE	∞
DOC. POSIZIONE TRIBUTARIA	∞
DOC. PRESA DI SERVIZIO	∞
DOC. PRODOTTA PER CONCILIAZIONE	∞
DOC. PRODOTTO DA ALUNNI PER ATT. DIDATTICHE	∞
DOC. PRODOTTO DA DOCENTI PER ATT. DIDATTICHE	∞
DOC. PRODOTTO DA DOCENTI PER PROGETTO FORMATIVO	∞
DOC. PRODOTTO DA DOCENTI PER SPERIMENTAZIONE MULTISCIPLINARE	∞
DOC. PRODOTTO DA STUDENTI PER PROGETTO FORMATIVO	∞
DOC. PRODOTTO DA STUDENTI PER SPERIMENTAZIONE MULTISCIPLINARE	∞
DOC. PROGETTI FORMATIVI	∞
DOC. PROGETTI FORMATIVI DI RECUPERO	∞
DOC. PROGETTO INVALSI	∞
DOC. RELATIVA A IMMOBILI DI PROPRIETA'	∞
DOC. RELATIVA A SCIOPERI	∞

DOC. RELATIVO A ATT. FORMATIVA O PARASCOLASTICA	∞
DOC. RELATIVO A ATTREZZAURE PER IMMOBILI DI PROPRIETA'	∞
DOC. RELATIVO A BORSA DI STUDIO	∞
DOC. RELATIVO A CESSIONE DEL QUINTO	∞
DOC. RELATIVO A CONTRATTAZIONE D'ISTITUTO	∞
DOC. RELATIVO A CONVENZIONI PER ATTIVITA' FORMATIVE E/O PARASCOLASTICHE	∞
DOC. RELATIVO A CONVENZIONI PER EDUCAZIONE ALLA SALUTE	∞
DOC. RELATIVO A EDUCAZIONE ALLA SALUTE	∞
DOC. RELATIVO A GRUPPI DI LAVORO OO.CC.	∞
DOC. RELATIVO A IMMOBILI DI PROPRIETA'	∞
DOC. RELATIVO A IMMOBILI IN USO	∞
DOC. RELATIVO A INAUGURAZIONI	∞
DOC. RELATIVO A INCHIESTA AMBIENTALI SOCIO/ECONOMICHE	∞
DOC. RELATIVO A MALATTIA PROFESSIONALE	∞
DOC. RELATIVO A MONITORAGGIO	∞
DOC. RELATIVO A PATRONATO SCOLASTICO	∞
DOC. RELATIVO A PENSIONE	∞
DOC. RELATIVO A PERCORSO DIDATTICO PRODOTTO DA DOCENTI	∞
DOC. RELATIVO A PERCORSO DIDATTICO PRODOTTO DA STUDENTI	∞
DOC. RELATIVO A PROGETTI DI EDUCAZIONE ALLA SALUTE	∞
DOC. RELATIVO A PROGETTI FORMATIVI	∞
DOC. RELATIVO A PROGETTI FORMATIVI TEATRALI	∞
DOC. RELATIVO A PROGETTI TRIMESTRALI O QUADRIMESTRALI	∞
DOC. RELATIVO A PROGETTO FORMATIVO MUSICALE	∞
DOC. RELATIVO A PROGETTO FORMATIVO ORIENTAMENTO	∞
DOC. RELATIVO A RAPPORTI CON ORGANIZZAZIONE SINDACALE	∞
DOC. RELATIVO A RAPPRESENTANZE SINDACALI INTERNE	∞
DOC. RELATIVO A RISTRUTTURAZIONE IMMOBILE	∞
DOC. RELATIVO A STAGE	∞
DOC. RELATIVO A STAGE	∞
DOC. RELATIVO A STATO DI FAMIGLIA	∞
DOC. RELATIVO A TRASFORMAZIONE SCUOLA	∞
DOC. RELATIVO A TRATTATO DI QUIESCENZA	∞
DOC. RISCATTO PERIODO ASSICURATIVO	∞
DOC. VALUTAZIONE RISCHI	∞
DOC. VISITA COLLEGIALE	∞
DOC. VISITA FISCALE	∞
DOCUMENTAZIONE INFORTUNIO	∞
DOCUMENTO PRODOTTO DA DOCENTI PER SUSSIDI	∞
DOCUMENTO PRODOTTO DA STUDENTI PER SUSSIDI	∞
DOCUMENTO PROGRAMMATICO SICUREZZA	∞
DOMANDA DI SCATTO ANTICIPATO	∞
DOMANDA DI TRASFERIEMENTO	∞
DONAZIONE IMMOBILE	∞
ELABORATI DEGLI ALUNNI	∞
ELABORATO PROVA SCRITTA O GRAFICA DI ESAME	∞
ELENCO DI CONSISTENZA BENE INVENTARIATO	∞
ELENCO PERSONALE	∞
FASCICOLO ATA	∞
FASCICOLO PERSONALE ALUNNO	∞
FASCICOLO PERSONALE DOCENTE	∞
GARANZIA APPARECCHIATURE	∞
GIORNALE DI CASSA	∞
GIORNALINO DI CLASSE	∞

INVENTARIO PATRIMONIALE BENI	∞
LETTERA DI INVITO AL DIPENDENTE	∞
LIBRETTO SCOLASTICO	∞
LIBRO GIORNALE CASSA SCOLASTICA	∞
LOCANDINA STAMPATA O PUBBLICATA DA O PER CONTO DELLA SCUOLA	∞
MODELLO 01/M	∞
MODELLO 101	∞
MODELLO CUD	∞
MODLELLO 26 CG	∞
NOMINA A COMMISSIONE OO.CC.	∞
NOMINA A GRUPPO DI LAVORO	∞
NOMINA COMITATO SCOLASTICO	∞
NORME ARCHIVIO SCOLASTICO	∞
NORME BIBLIOTECA	∞
ORARIO DELLE LEZIONI	∞
ORDINANZA INTERNA	∞
ORDINE DI SERVIZIO GENERALE	∞
PAGELLA SCOLASTICA	∞
PARTITARIO ENTRATE	∞
PEI	∞
PERMESSO BREVE DEL PERSONALE	∞
PERMESSO DI STUDIO DEL PERSONALE	∞
PIANO DI LAVORO	∞
PIANTA ORGANICA	∞
PLANIMETRIA IMMOBILE DI PROPRIETA'	∞
PLANIMETRIA IMMOBILE IN USO	∞
POF	∞
PON	∞
POR	∞
PORTFOLIO	∞
PRATICA PER ASSISTENZA COLONIA	∞
PROGETTO TECNICO	∞
PROGETTO TECNICO IMPIANTI O ATTREZZATURE	∞
PROGRAMMA CONTABILE ANNUALE	∞
PROGRAMMA D'ESAME	∞
PROGRAMMA DOCENTE	∞
PUBBLICAZIONE VARIA DELLA SCUOLA	∞
QUESTIONARIO	∞
RASSEGNA STAMPA SCUOLA	∞
RAV	∞
REFERTO VISITA COLLEGIALE	∞
REFERTO VISITA FISCALE	∞
REGISTRIO CRONOLOGICO DEI CONTRATTI	∞
REGISTRO CARICO E SCARICO DEI DIPLOMI	∞
REGISTRO CONSEGNA DIPLOMI	∞
REGISTRO CONTRATTI FORNITURA MATERIALE	∞
REGISTRO DEI CERTIFICATI	∞
REGISTRO DEI CONTRATTI	∞
REGISTRO DEI VERBALI OO.CC.	∞
REGISTRO DELIBERAZIONI	∞
REGISTRO DI CLASSE	∞
REGISTRO DI ENTRATA BIBLIOTECA	∞
REGISTRO DI ENTRATA SUSSIDI MULTIMEDIALI	∞
REGISTRO DI STATO DEL PERSONALE	∞
REGISTRO GENERALE DEI VOTI	∞
REGISTRO INFORTUNI	∞

REGISTRO ISCRIZIONE ALUNNI	∞
REGISTRO LICENZE SOFTWARE	∞
REGISTRO MODELLI AT	∞
REGISTRO OPERAZIONI CONTO CORRENTE BANCARIO	∞
REGISTRO OPERAZIONI CONTO CORRENTE POSTALE	∞
REGISTRO PROFILO ALUNNO	∞
REGISTRO PROTOCOLLO	∞
REGISTRO RIUNIONI PER DIPARTIMENTO	∞
REGISTRO RIUNIONI PER MATERIA	∞
REGISTRO SPESE PER APERTURA CREDITO	∞
REGISTRO STIPENDI	∞
REGISTRO STIPENDI	∞
REGISTRO VERBALI CASSA SCOLASTICA	∞
REGISTRO VERBALI CONSIGLIO DI AMMINISTRAZIONE	∞
REGISTRO VERBALI CONTRATTAZIONE D'ISTITUTO	∞
REGISTRO VERBALI DEL COLLEGIO DEI REVISORI	∞
REGISTRO VERBALI ESAME DI STATO	∞
REGISTRO VERBALI PROVE D'ESAME	∞
REGOLAMENTO BIBLIOTECA	∞
REGOLAMENTO INTERNO LABORATORIO	∞
REL. COLL.NE ASSOCIAZIONI E COOPERATIVE	∞
RELAZIONE ADOZIONE LIBRO DI TESTO	∞
RELAZIONE COLLABORAZIONE ENTE LOCALE	∞
RELAZIONE COLLABORAZIONE ESPERTO ESTERNO	∞
RELAZIONE COLLABORAZIONE ISTITUZIONI SOCIO ASSISTENZIALI	∞
RELAZIONE CONSULENZA SSN	∞
RELAZIONE CONSULENZA TRIBUNALE DEI MINORI	∞
RELAZIONE ESTERNA	∞
RELAZIONE FINALE DI CLASSE	∞
RELAZIONE FINALE D'ISTITUTO	∞
RELAZIONE RIPETENZA ALUNNI	∞
RELAZIONE SU COLLABORAZIONE COOP. E ASSOCIAZIONI	∞
RELAZIONE SU COLLABORAZIONE SSN	∞
RELAZIONE SU CONSULENZE COOP. E ASSOCIAZIONI	∞
RELAZIONECOLLABORAZIONE TRIBUNALE DEI MINORI	∞
RENDICONTO TRIMESTRALE	∞
REPERTORIO D'ARCHIVIO	∞
REPERTORIO FASCICOLI D'ARCHIVIO	∞
RICOGNIZIONE PATRIMONIALE DECENNALE	∞
RICOGNIZIONE PATRIMONIALE DI SCUOLA CONFLUITA	∞
RICORSO AMMINISTRATIVO	∞
RIVALUTAZIONE PATRIMONIALE QUINQUENNALE	∞
RSU	∞
RUBRICA ALFABETICA DEL PROTOCOLLO	∞
RUOLO DEL PERSONALE	∞
SCHEDA ALUNNO	∞
SCHEDARIO ALUNNI	∞
STATISTICA	∞
STATO DI FAMIGLIA	∞
STATUTO E REGOLAMENTO	∞
TESSERA MINISTERIALE	∞
TITOLO DI STUDIO	∞
TRATTAMENTO QUIESCENZA	∞
VERBALE ADOZIONE LIBRI DI TESTO	∞
VERBALE CASSA SCOLASTICA	∞
VERBALE COMITATO SCOLASTICO	∞

VERBALE COMMISSIONE ELETTORALE OO.CC.	∞
VERBALE COMMISSIONE OO.CC.	∞
VERBALE CONSIGLIO DI AMMINISTRAZIONE E DI PRESIDENZA	∞
VERBALE CONTRATTAZIONE D'ISTITUTO	∞
VERBALE DEL COLLEGIO DEI REVISORI	∞
VERBALE DI COLLAUDO	∞
VERBALE DI COLLAUDO ATTREZZATURA	∞
VERBALE DI CONSEGNA BENE INVENTARIATO	∞
VERBALE GRUPPO DI LAVORO OO.CC.	∞
VERBALE ISPETTORI SCOLASTICI	∞
VERBALE ORGANO COLLEGIALE	∞
VERBALE PASSAGGIO DI CONSEGNA	∞
VERBALE PROVA D'ESAME	∞
ACCONTO AL PERSONALE	50
ATTO COSTITUTIVO COLLEGIO REVISORI	50
ATTO RELATIVO A LOCAZIONE IMMOBILI	50
CONTRATTO DI PRESTAZIONE D'OPERA	50
DENUNCIA ANNUALE IRAP	50
DENUNCIA MENSILE ANALITICA	50
DENUNCIA RETRIBUTIVA MENSILE	50
DISPOSIZIONE CCNL	50
DISPOSIZIONE PERSONALE	50
DOC. COMPENSO A VARIO TITOLO	50
DOC. CONGUAGLIO PER IL PERSONALE	50
DOC. FONDO ESPERO	50
DOC. PER CONSULENZA LIQUIDAZIONE	50
DOC. REGOLARIZZANTE CONTRIBUTIVA PERSONALI	50
DOC. RELATIVO A CONTRIBUTI INPS	50
DOC. RELATIVO A RECUPERO RETRIBUZIONE	50
EMENS	50
MODELLO 770	50
NORMA CCNL	50
REGISTRO ASSENZE PERSONALE	50
TABELLA STIPENDIO	50
TABULATO MENSILE RIEPILOGATIVO RETRIBUZIONE	50
TABULATO RIEPILOGATO IMPONIBILE	50
ACQUISTO ATTREZZATURA	10
BOLLETTARIO CARICO SCARICO	10
BOLLETTINO CC/POSTALE	10
BUONO D'ORDINE	10
COPIA DELIBERA LIQUIDAZIONE	10
COPIA DETERMINA DI LIQUIDAZIONE	10
COPIA DI DELIBERE DI LIQUIDAZIONE	10
CORRISPONDENZA RELATIVA A ACQUISTI	10
CORRISPONDENZA RELATIVA A INTERVENTI DI MANUTENZIONE	10
DISTINTA TRASMISSIONE AL TESORIERE MANDATI	10
DISTINTA TRASMISSIONE AL TESORIERE REVERALI	10
DISTINTA TRASMISSIONE TESORERIA	10
DO. RELATIVA A REVERSALE DI PAGAMENTO	10
DOC. GIUSTIFICATIVO A MANDATO DI PAGAMENTO	10
DOC. RELATIVA A CERIMONIA	10
DOC. RELATIVA A INTERVENTI DI MANUTENZIONE	10
DOC. RELATIVA A NOMINA CASSIERE ISTITUTO	10
DOC. RELATIVA A RECUPERO ORARIO	10
ELENCO ALUNNI	10
ESTRATTO CONTO BANCARIO	10
ESTRATTO CONTO POSTALE	10

FATTURA	10
FOGLIO DI PRESENZA	10
GRADUATORIA D'ISTITUTO	10
GRADUATORIA NON IN VIGORE	10
LICENZA SOFTWARE	10
MANDATO DI PAGAMENTO	10
ORDINATIVO ACQUISTO	10
REGISTRO ATTIVITA' GRUPPO SPORTIVO	10
REGISTRO DEBITI FORMATIVI	10
REGISTRO POSTA IN PARTENZA E IN ARRIVO	10
REGISTRO TASSE SCOLASTICHE PER ISCRIZIONE E DIPLOMA	10
REVERSALE DI PAGAMENTO	10
UTENZA ELETTRICA	10
UTENZA TASSA RIFIUTI	10
UTENZA TELEFONO	10
VERBALI DEBITO FORMATIVO	10
ABB. A GIORNALE	6
ABB. A PUBBLICAZIONE	6
ABB. A RIVISTA	6
ACQUISTO GIORNALE	6
ACQUISTO LIBRI	6
ACQUISTO MATERIALE DI CONSUMO	6
ACQUISTO PUBBLICAZIONE	6
ACQUISTO RIVISTA	6
ATTESTAZIONE PAGAMENTO SERVIZIO DI TRASPORTO	6
AUTORIZZAZIONE ALL'USO DI IMPIANTI SPORTIVI	6
AUTORIZZAZIONE USO LOCALI SCOLASTICI	6
BOLLETTARIO RICHIESTA STAMPATI	6
BUONI LIBRI, DOC. DI SUPPORTO	6
BUONO LIBRO	6
CEDOLA LIBRARIA	6
CERTIFICATO NASCITA	6
CERTIFICATO NASCITA E VACCINAZIONE ALUNNO	6
CERTIFICATO VACCINAZIONE	6
CONVOCAZIONE RIUNIONE OO.CC.	6
COPIA DI CERTIFICATO	6
DOC. PRODOTTA DA CANDITATO A ESAME	6
DOC. RELATIVA A GITE SCOLASTICHE	6
DOC. RELATIVI A CAMPAGNE DI DISINFESTAZIONE/VACCINAZIONE	6
DOC. RELATIVO A MANFESTAZIONE TEATRALE	6
DOC. RELATIVO A ATTIVITA' SCOLASTICA ESTERNA	6
DOC. RELATIVO A ATTIVITA' SCOLASTICA INTERNA	6
DOC. RELATIVO A BUONI ACQUISTI GENERE DI REFEZIONE E CONSUMO	6
DOC. RELATIVO A CAMPAGNE DISINFESTAZIONE	6
DOC. RELATIVO A CAMPAGNE VACCINAZIONE	6
DOC. RELATIVO A CONTRIBUTI ALLA BIBLIOTECA SCOLASTICA	6
DOC. RELATIVO A CONTRIBUTI BIBLIOTECA	6
DOCUMENTI PER ISCRIZIONI	6
DOMANDA AMMISSIONE A ESAME	6
DOMANDA ISCRIZIONE	6
ELENCO BUONI LIBRI CONCESSI	6
ELENCO PRESENZE MENSA	6
LIBRETTO AUTOMOBILE	6
MATRICE DI BUONI ACQUISTO PER GENERI DI REFEZIONE E	6

CONSUMO	
NOMINA OO.CC	6
REGISTRO ASSENZE ALUNNI	6
REGISTRO ELZIONE PRIVATE	6
RICHIESTA CONSULTAZIONE ARCHIVIO	6
RICHIESTA DI CERTIFICATO	6
RICHIESTA DI FERE	6
RICHIESTA DI INTERVENTO	6
RICHIESTA DI RISORSE STRUMENTALI	6
RICHIESTA DI TRASPORTO GRATUITO	6
RICHIESTA INTERVENTO DOTAZIONE STRUMENTALE	6
RICHIESTA ISCRIZIONE MENSA	6
RICHIESTA ISCRIZIONE SERVIZIO DI TRASPORTO ALUNNI	6
RICHIESTA STAMPATI	6
VISITA DI STUDIO	6
ABB. FERROVIARIO O DIVERSO	1
COMPITO IN CLASSE	1
ELABORATO PROVE PRATICA ESAME	1
GRADUATORIA IN CALCE	1
REGISTRO IMMATRICOLAZIONE ALUNNI	1
RICHIESTA ACCESSO A DOCUMENTI	1
RICHIESTA COPIA DI ATTI	1
RISCHIESTA SUPPLENZA	1

MODULO DI CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELL'ARCHIVIO

Spett.le Dirigente Scolastico
IC VILLONGO

Oggetto: Richiesta di consultazione del materiale documentario conservato nella sezione di deposito/storica dell'Archivio generale dell'Amministrazione.

Scopo della consultazione:
.....
.....
.....
.....

Durata indicativa della consultazione: ..... mesi

Materiale da consultare:

o **Titolo**
.....

o **Classe**
.....

o **Sottoclasse**
.....

o **Descrizione dei fascicoli:**

- Oggetto del fascicolo:
.....
.....
- Anno di repertoriazione
.....
- Dal numero ..... al numero
.....

o **Descrizione dei sottofascicoli:**

- Oggetto del fascicolo:
.....
.....
- Anno di repertoriazione
.....
- Dal numero ..... al numero
.....

o **Descrizione degli inserti:**

- Oggetto del fascicolo:
.....
.....
- Anno di repertoriazione
.....

- Dal numero ..... al numero .....

NOTE:

.....
..
.....
.....

lì .....

L'OPERATORE RICEVENTE:

.....

IL RESPONSABILE DELL'ARCHIVIO:

.....

NOMINA DEL RESPONSABILE DEL SERVIZIO ARCHIVISTICO

Determinazione n.°25 del 31/04/2015

Oggetto: **Nomina del Responsabile del Servizio archivistico**

L'anno 2015 , il giorno 31 del mese di marzo , nell'amministrazione IC VILLONGO sita in VILLONGO -

IL DIRIGENTE

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che il sistema di gestione informatica dei documenti deve garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato, art. 52, comma 1 lettera f) del testo unico;

CONSIDERATO inoltre la materia trattata richiede conoscenze e competenze specifiche; **VISTA** la determinazione numero 25 del 31/04/2015 relativa alla nomina del Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;

RITENUTO di individuare nel/nella signor/signora SOCIETA' DADONET S.A.S., in carico presso l'Ufficio Utente IC Villongo , la figura professionale più idonea ad espletare i compiti di seguito indicati:

- collaborare con il Responsabile del servizio per la tenuta del protocollo e la gestione documentale per:

– predisporre lo schema del Manuale di gestione,

– stabilire i criteri minimi di sicurezza informatica del sistema,

– organizzare il sistema di gestione dei flussi documentali e la classificazione dei documenti, lo smistamento e l'assegnazione dei documenti alle UOR (sulla scorta dell'organigramma dell'Amministrazione), la costituzione e la repertoriazione dei fascicoli, l'individuazione dei responsabili della conservazione dei documenti e dei fascicoli nella fase corrente,

– stabilire i livelli di accesso ai documenti archivistici e regolamentare le forme di

consultazione interna ed esterna dell'archivio, nel rispetto della normativa sulla tutela della riservatezza dei dati personali, con particolare riferimento all'allegato "A.2 Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" del d. lgs. 196/03;

- organizzare la fase di versamento dei documenti dagli uffici all'Archivio generale, insieme con gli strumenti di corredo, e predisporre l'elenco dei fascicoli e delle serie ricevute;
- curare e garantire la conservazione dell'archivio nella fase di deposito;
- predisporre il piano di conservazione dei documenti, prescritto dal DPR 445/2000, art. 68;
- predisporre il massimario di scarto;
- effettuare la selezione periodica dei documenti e procedere allo scarto o al trasferimento nella separata sezione d'archivio del materiale destinato alla conservazione permanente.

DETERMINA

1. di nominare il/la signore/a SOCIETA' DADONET S.A.S. quale Responsabile del Servizio archivistico con i compiti specificati nelle premesse.

IL DIRIGENTE SCOLASTICO

Prof.ssa Maria Luisa Mastrogiovanni

Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del d.lgs. n.39/1993

NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE SOSTITUTIVA

Determinazione n. 199 del 28/12/2015

Oggetto: **Nomina del Responsabile del Servizio di conservazione sostitutiva**

L'anno 2015 , il giorno 28 del mese di dicembre, nell'amministrazione IC VILLONGO sita in VILLONGO - via Volta,1

IL DIRIGENTE

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che il sistema di gestione informatica dei documenti deve garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;

VISTO l'art. 62 comma 1 del DPR n. 445/2000 concernente le procedure di salvataggio e conservazione delle informazioni del sistema di gestione elettronica dei documenti;

VISTA la determinazione numero 199 del 28/12/2015 relativa alla nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;

VISTO l'art. 2 comma 2 del Codice dell'amministrazione digitale (Dlgs 7 marzo 2005, n. 82) sulla applicazione del codice a tutte le pubbliche amministrazioni di cui all'art. 1, comma 2 del Dlgs 30 marzo 2001, n. 165, "ivi compresi gli istituti e scuole di ogni ordine e grado"

PRESO ATTO che il sottoscritto in qualità di Dirigente dell'Istituto assume la qualifica di "Responsabile della Conservazione" ai sensi dell'art. 7 comma 3 del DPCM 3 dicembre 2013;

CONSIDERATO che Il Responsabile sopra richiamato intende delegare le attività operative di conservazione sostitutiva dei documenti digitali dell'Amministrazione che rappresenta a soggetto diverso da se medesimo;

PRESO ATTO che questo ufficio, per la gestione della Segreteria digitale, ha software "Nuvola" della MADISOFT SPA le cui condizioni Generali di contratto sono allegate al modulo di attivazione prot. n.° 277 /A24c del 19 /01/2016;

PRESO ATTO che la MADISOFT S.P.A. è Partner della Aruba PEC S.P.A. per la fornitura del servizio di Conservazione sostitutiva denominato "DocFly" ai clienti del Partner ;

RITENUTO di delegare la società Aruba PEC S.P.A. quale "Responsabile del servizio di

conservazione" dei documenti informatici della tipologia riportata nelle schede di conservazione allegate al Contratto definito "Servizi DocFly cliente Partner" al fine di:

• rendere le informazioni trasferite sempre consultabili;

• provvedere alla conservazione degli strumenti hardware e software atti a garantire la consultabilità dei documenti conservati;

• eseguire, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici rimovibili.

DETERMINA

• di individuare il responsabile del servizio di conservazione dei documenti informatici nella società Aruba PEC S.P.A

• di individuare nel Direttore dei Servizi Generali e Amministrativi il funzionario tenuto alla vigilanza sugli adempimenti connessi alla gestione documentale e agli archivi per quanto compreso nei compiti connessi al profilo di appartenenza.

• di rendere il presente decreto immediatamente esecutivo con la richiesta di Erogazione servizi DOCFLY Cliente Partner.

IL DIRIGENTE SCOLASTICO

Prof.ssa Maria Luisa Mastrogiovanni

Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del d.lgs. n.39/1993

ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Determinazione n. 5036 del 27/09/2016

Oggetto: **Nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e del suo Vicario.**

L'anno 2016, il giorno 27 del mese di settembre, nell'amministrazione IC VILLONGO sita in VILLONGO – Via Volta,1

IL DIRIGENTE

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi e delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

VISTO in particolare l'articolo 61, comma 2, il quale tra l'altro, stabilisce che presso il servizio gratuito del protocollo informatico, è preposto un dirigente, ovvero un funzionario, comunque in possesso di idonei requisiti professionali e di professionalità tecnico archivistica;

VISTO il Decreto ministeriale 14 ottobre 2003 "Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi", nel quale sono indicati gli adempimenti delle amministrazioni relativamente al protocollo informatico ed alla gestione dei procedimenti amministrativi con tecnologie informatiche;

RITENUTO di individuare nel/nella signor/signora GANDOSSI LUCIA CRISTINA, in carico presso l'Ufficio Utente IC Villongo, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale anche su Internet;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il:

– Responsabile dei sistemi informativi automatizzati,

– Referente della pianificazione delle attività,

– Responsabile della sicurezza dei dati personali, se nominato, o direttamente con il Titolare dei trattamenti dei dati di cui al d. lgs. 196/03,

– Responsabile del servizio archivistico,

– Responsabile della conservazione sostitutiva;

- attribuire il livello di autorizzazione di ciascun addetto all'accesso alle funzioni delle procedure applicative di gestione del protocollo informatico e gestione documentale distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento, alla modifica e alla cancellazione delle informazioni;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;
- curare, anche attraverso altri responsabili, le funzionalità del sistema di gestione informatica del protocollo e della gestione documentale affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conservare le copie di salvataggio delle informazioni del sistema e del registro di emergenza in luoghi sicuri differenti;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso esterno o da altre Amministrazioni e le attività di gestione degli archivi, quali, trasferimento dei documenti all'archivio di deposito, disposizioni per la conservazione degli archivi e Archivi storici;
- autorizzare le operazioni di annullamento della registratura di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme correnti da parte del personale autorizzato e degli incaricati.

DETERMINA

2. di nominare il/la signore/a GANDOSSI LUCIA CRISTINA quale Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ai sensi dell'articolo 61 comma 2 del DPR n. 445/2000 con i compiti specificati nelle premesse.
3. di nominare vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per i casi di vacanza, assenza o impedimento del Responsabile, viene nominato il/la signor/signora DSGA.

IL DIRIGENTE SCOLASTICO

Prof.ssa Maria Luisa Mastrogiovanni

Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del d.lgs. n.39/1993

POLITICHE DI SICUREZZA

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATICO

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, l'Intranet, la Extranet 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.

3. 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.

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.

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/e ditta/e < *inserire nome* > , 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.

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 o Divisioni o Direzioni, 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.

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.

2. 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 quattro 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.

2 Politiche Antivirus

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.

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.

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.

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

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.

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.

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.

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).

4 LINEE TELEFONICHE COMMUTATE (ANALOGICHE E DIGITALI)

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.

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.

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.

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.

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.

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;
- che cosa la connessione esterna richiede per essere acceduta.

5 POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

5.1 Scopo

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

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.

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.

6 POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA

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.

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.

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.

7 POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

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.

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.

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.

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.
4. Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

8 POLITICHE PER LE COMUNICAZIONI WIRELESS

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.

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.

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.

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.

PIANO FORMATIVO PER IL PERSONALE

Amministrazione IC VILLONGO

PER IL PERSONALE DELL'AREA ORGANIZZATIVA OMOGENEA RICHIAMATA I PIANI FORMATIVI PREVISTI SONO QUELLI STESSI DEFINITI CON NOTA DEL 22/12/2016, PROTOCOLLO 40587, AVENTE AD OGGETTO: Piano di formazione per il personale ATA a.s. 2016-17, PER IL MINISTRO DELLA FUNZIONE PUBBLICA SULLA FORMAZIONE E LA VALORIZZAZIONE DEL PERSONALE DELLE PUBBLICHE AMMINISTRAZIONI, QUI DI SEGUITO RICHIAMATI:

Gli argomenti dei corsi per l'area A possono riguardare:

- l'accoglienza e la vigilanza e la comunicazione;
- l'assistenza agli alunni con disabilità;
- la partecipazione alla gestione dell'emergenza e del primo soccorso.

Gli argomenti dei corsi per l'area B (profilo amministrativo) possono riguardare:

- il servizio pubblico: dalla cultura dell'adempimento alla cultura del risultato;
- i contratti e le procedure amministrativo-contabili (fatturazione elettronica, gestione della trasparenza e dell'albo-online, protocolli in rete, neoassunti, etc.);
- le procedure digitali sul SIDI;
- la gestione delle relazioni interne ed esterne;
- le ricostruzioni di carriera e i rapporti con le ragionerie territoriali.

Gli argomenti dei corsi per l'area B (profilo tecnico) possono riguardare:

- la funzionalità e la sicurezza dei laboratori;
- la gestione dei beni nei laboratori dell'istituzione scolastica;
- la gestione tecnica del sito web della scuola;
- il supporto tecnico all'attività didattica per la propria area di competenza;
- la collaborazione con gli insegnanti e con i dirigenti scolastici nell'attuazione dei processi di
- innovazione dell'istituzione scolastica (PNSD, PTOF, etc.).

.

Gli argomenti dei corsi per l'area D possono riguardare:

- autonomia scolastica: dalla cultura dell'adempimento alla cultura del risultato;
- la gestione del bilancio della scuola e delle rendicontazioni;
- le relazioni sindacali;
- la nuova disciplina in materia di appalti pubblici(Dlgs.50/2016) e gli adempimenti connessi con i progetti PON;
- la gestione delle procedure di acquisto attraverso il mercato elettronico (acquistinretepa.it);

- la disciplina dell'accesso alla luce delle recenti innovazioni normative (Trasparenza,FOIA,etc. Dlgs.33/2013 e successive modificazioni);
- la gestione dei conflitti e dei gruppi di lavoro;
- il proprio ruolo nell'organizzazione scolastica e la collaborazione con gli insegnanti e con il dirigente scolastico nell'ambito dei processi d'innovazione della scuola (organicodell'autonomia, piano nazionale di scuola digitale, PTOF, RAV, etc.);
- la gestione amministrativa del personale della scuola.

A seguito delle Indicazioni Ministeriali l'Istituto Comprensivo di Villongo ha previsto la formazione personale ATA come di seguito evidenziato:

	a.s. 2016/17	**a.s. 2017/2018**	**a.s. 2018/2019**
Collaboratori scolastici	Corso privacy. Corso digitalizzazione segreteria.	Corsi base ed avanzati di informatica.	Corsi base ed avanzati di informatica.
Personale ATA – DSGA e Assistenti amministrativi	Formazione sugli obblighi relativi alla riservatezza e protezione dei dati personali (cd *privacy*); Formazione sugli obblighi di pubblicità e trasparenza nella gestione dei documenti e del sito d'Istituto, con particolare riguardo all'Albo on line e alla sezione "Amministrazione trasparente". Corsi di formazione/aggiornamento per le specifiche competenze degli Assistenti (gli appalti pubblici dopo le riforme del 2014; gli acquisti con MEPA; le assenze del personale…).	Aggiornamento sugli obblighi relativi alla riservatezza e protezione dei dati personali (cd *privacy*); Aggiornamento sugli obblighi di pubblicità e trasparenza nella gestione dei documenti e del sito d'Istituto, con particolare riguardo all'Albo on line e alla sezione "Amministrazione trasparente". Corsi di formazione/aggiornamento per le specifiche competenze degli Assistenti	I reati contro la Pubblica Amministrazione corsi di formazione/aggiornamento per le specifiche competenze degli Assistenti

NORMATIVA DI RIFERIMENTO

1. *Legge 7 agosto 1990*, n. 241 Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. del 18 agosto 1990, n. 192)
2. *DPR 27 giugno 1992*, n. 352 Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. 29 luglio 1992, n. 177)
3. *DPR 12 febbraio 1993*, n. 39 Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera m), della legge 23 ottobre 1992, n. 421. (G.U. 10 febbraio 1993, n. 42)
4. *Legge 15 marzo 1997*, n. 59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa.
5. *DPCM 28 ottobre 1999* Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290)
6. *Decreto legislativo 29 ottobre 1999*, n. 490 Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352. (G.U. 27 dicembre 1999, n. 302)
7. *DPCM 31 ottobre 2000* Regole tecniche per il protocollo informatico; valido ai sensi dell'art. 78 del DPR 28 dicembre 2000, n. 445. (G.U. n. 272 del 21 novembre 2000)
8. *Deliberazione AIPA 23 novembre 2000*, n. 51Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del DPR 10 novembre 1997, n. 513. (G.U. 14 dicembre 2000, n. 291)
9. *DPR 28 dicembre 2000*, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42)
10. *Circolare del 16 febbraio 2001*, n. AIPA/CR/27 – "Art. 17 del DPR 10 novembre 1997, n. 513 Utilizzo della firma digitale nelle pubbliche amministrazioni".
11. *Decreto legislativo 30 marzo 2001*, n. 165 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche".
12. *Circolare AIPA 7 maggio 2001*, n. AIPA/CR/28 Articolo 18, comma 2, del DPCM 31 ottobre 2000 recante regole tecniche per il protocollo informatico di cui al DPR 28 dicembre 2000, n. 445 Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati. (G.U. 21 novembre 2000, n. 272)
13. *Circolare AIPA 21 giugno 2001*, n. AIPA/CR/31 (Art. 7, comma 6, del DPCM 31 ottobre 2000 recante "Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428" requisiti minimi di sicurezza dei sistemi operativi disponibili.)
14. *Direttiva del Ministro per la funzione pubblica del 13 dicembre 2001* Formazione del personale. (G.U. del 31 gennaio 2002, n. 26)
15. *Direttiva 16 gennaio 2002*, Dipartimento per l'innovazione e le tecnologie Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali.
16. *Decreto legislativo 23 gennaio 2002*, n. 10 Recepimento della direttiva 1999/93/CE sulla firma elettronica.

17. *Direttiva del Ministro per l'innovazione e le tecnologie, 9 dicembre 2002* -Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
18. *Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre* 2002 Linee guida in materia di digitalizzazione dell'amministrazione.
19. *Legge 27 dicembre 2002*, n. 289 Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
20. *DPR 7 aprile 2003,* n. 137 Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002.
21. *Decreto legislativo 30 giugno 2003*, n. 196 Codice in materia di protezione dei dati personali.
22. *Decreto Ministeriale 14 ottobre 2003* Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)
23. *Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre* 2003 Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8)
24. *Direttiva 1999/93/CE del Parlamento europeo e del consiglio del 13 dicembre 2003.*
25. *Direttiva 18 dicembre 2003* Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28)
26. *DPCM 13 gennaio 2004* Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. 27 aprile 2004, n. 98)
27. *Deliberazione CNIPA 19 febbraio 2004*, n. 11 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
28. *Decreto legislativo 22 gennaio 2004*, n. 42 Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137. (G.U. 24 febbraio 2004, n. 28).
29. *L. 28 gennaio 2009, n. 2* Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (estratto relativo alla PEC)
29. *DPCM 30 marzo 2009* Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
30. *L. 18 giugno 2009, n. 69* Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile (estratto relativo all'Amministrazione digitale)
29. *DECRETO LEGISLATIVO 30 dicembre 2010*, n. 235 Modifiche ed integrazioni al decreto legislativo 7 Marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. (11G0002) (GU n.6 del 10-1-2011 - Suppl. Ordinario n. 8)
30. *DPCM 22 luglio 2011* Comunicazioni Imprese PA
31. *Circolare AGID del 23 gennaio 2013, n 60* Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni.
32. *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario;
32. *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 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 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario;

33. *Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014* - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015;

ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE

NOMINATIVO	TITOLO/RUOLO NELL'AOO	ESTREMI E DESCRIZIONE DELLA DELEGA RICEVUTA
Maria Luisa Mastrogiovanni	Dirigente	
Annalisa Fiumi	D. S. G. A.	