Comune di Villanova Monferrato (AL)

Documento Misure Minime di Sicurezza ICT e Trattamento Dati

Direttiva del 1° agosto 2015 del Presidente del Consiglio del Ministri sulla protezione cibernetica e la sicurezza informatica

Misure minime di sicurezza ICT per le Pubbliche Amministrazioni emana te da AGID (Agenzia per l'Italia Digitale), contenute nella Circolare n. 2/2017 del 18 aprile 2017, pubblicata in Gazzetta Ufficiale il 5 maggio 2017 con numero generale 103, in sostituzione della Circolare n.1/2017.

Sommario

Premessa **pag. 3**

Riferimenti normativi **pag. 5**

Figure rilevanti ai sensi **pag. 6**
D.Lgs. 196/2003 (art.4) e Regolamento UE 679/2016 (art.4)

Figure rilevanti ai sensi **pag. 9**
D.Lgs. 179/2016 (art.17)

Analisi dei rischi **pag. 9**

Valutazione del livello di sicurezza **pag. 11**

Analisi della situazione comunale **pag. 25**
Aspetti logistici e trattamento dati in formato elettronico: strumenti e dotazioni informatiche a)

Aspetti logistici e trattamento dati in formato non elettronico: strumenti e dotazioni b)

Modulo di implementazione delle misure minime di sicurezza nelle pubbliche amministrazioni **pag. 26**

Modalità di aggiornamento **pag. 26**

PREMESSA

Il presente documento è redatto in ottemperanza a quanto richiesto dalla Direttiva del 1° agosto 2015 del Presidente del Consiglio del Ministri sulla protezione cibernetica e la sicurezza informatica, secondo la quale "*Occorre proseguire con determinazione nell'attuazione degli indirizzi strategici ed operativi identificati, ponendo in essere tutte le linee di azione necessarie sotto il profilo tecnico, organizzativo, procedurale e della collaborazione internazionale, che consentano di assicurare ai nostri cittadini uno spazio cibernetico in cui possano essere esercitate, in una cornice di sicurezza, diritti fondamentali",* questi ultimi definiti dal D.Lgs. 179/2016 ovvero il Codice dell'Amministrazione Digitale, art. 3 "Diritto all'uso delle tecnologie".
La Direttiva evidenzia la necessità di fissare linee di azione precise per la sua attuazione ovvero *"tutte le Amministrazioni devono dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad aventi cibernetici".*

Al fine di agevolare tale processo, AGID (l'Agenzia per l'Italia Digitale) ha attuato la Direttiva emanando le **Misure minime di sicurezza ICT per le Pubbliche Amministrazioni**, contenute nella Circolare n. 2/2017 del 18 aprile 2017, pubblicata in Gazzetta Ufficiale il 5 maggio 2017 con numero generale 103, in sostituzione della Circolare n.1/2017.
Le Misure Minime forniscono alle Pubbliche Amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando soprattutto gli interventi obbligatori da compiere per l'adeguamento.
Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie o in sua assenza il dirigente allo scopo designato, ha la responsabilità dell'attuazione delle misure di cui all'art. 1 della suddetta circolare (art.3). Le modalità con cui ciascuna misura è implementata presso l'amministrazione devono essere riportate nel modulo di implementazione di cui all'allegato 2 della Circolare, che deve essere compilato, firmato digitalmente con marcatura temporale dal soggetto responsabile di cui all'art.3 e dal responsabile legale della Pubblica Amministrazione, conservato e, in caso di incidente informatico, trasmesso a CERT-PA (Computer Emergency Response Team, struttura che opera all'interno di AGID preposta al trattamento degli incidenti di sicurezza informatica) con la segnalazione dell'incidente stesso. (art.4).

Le Amministrazioni devono attuare gli adempimenti entro il 31 dicembre 2017 (art.5).

Il presente documento definisce, inoltre, l'organizzazione e l'attuazione dei principi e delle regole espresse nel Codice in materia di protezione dei dati personali, D.lg. 196/03 e s.m.i. e secondo le previsioni del relativo allegato B.
Il Codice prescrive precisi obblighi e comportamenti da attuare nel trattamento dei dati e nei criteri organizzativi interni da seguire per l'attuazione e per fornire idonee informazioni a riguardo, anche a parti terze.
I principi fondamentali che devono essere alla base di ogni trattamento di dati, intendendo così qualsiasi operazione effettuata con i dati stessi, dalla raccolta alla conservazione fino all'utilizzo e alla distruzione, riguardano la necessità e la liceità del trattamento e la sua effettuazione secondo correttezza, l'esattezza dei dati e l'aggiornamento degli stessi, la completezza e la pertinenza e quindi la non eccedenza rispetto alle finalità per le quali i dati
sono stati raccolti e successivamente trattati, la conservazione in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati.
Nel presente documento si definiscono anche le direttive contenute nel Regolamento europeo in materia di protezione dei dati personali.
Il 4 maggio 2016 infatti è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) il testo del suddetto Regolamento Europeo (Regolamento UE n. 679/2016), entrato ufficialmente in vigore il 24 maggio 2016 e che deve essere recepito dagli Stati membri dell'Unione entro 2 anni, quindi entro il 25 maggio 2018, obbligatoriamente anche in Italia.
È necessario che anche tutte le Pubbliche Amministrazioni si adeguino alle nuove direttive entro la data stabilita e quindi provvedano già da adesso a programmare i necessari interventi da adottare e le modalità con cui effettuare gli adeguamenti stessi.

RIFERIMENTI NORMATIVI

i. Circolare n. 2/2017 del 18 aprile 2017: Misure minime di sicurezza ICT per le Pubbliche Amministrazioni – AGID, Agenzia per l'Italia Digitale, pubblicato in Gazzetta Ufficiale Serie Generale n.103 del 5/5/2017 [revisione e sostituzione della Circolare AGID 1/2017 del 17 marzo 2017]

ii. Direttiva del 1° agosto 2015 del Presidente del Consiglio del Ministri sulla protezione cibernetica e la sicurezza informatica

iii. Decreto Legislativo 26 agosto 2016 n. 179, Codice dell'Amministrazione Digitale

iv. Regolamento eIDAS – Regolamento UE n. 910/2014

v. Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

vi. Decreto Legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali e s.m.i.

vii. Disciplinare tecnico in materia di misure minime di sicurezza del Decreto Legislativo 196/2003 (Codice delle Privacy - allegato B)

viii. Codice Penale, in particolare gli articoli introdotti con la Legge del 23 dicembre 2003 n. 547 (modifiche ed integrazioni alle norme del Codice Penale e del Codice di procedura penale in tema di criminalità informatica)

LE FIGURE RILEVANTI

D.Lgs. n. 196/2003 (art.4) e Regolamento UE 679/2016 (art.4)

a) TITOLARE DEL TRATTAMENTO

Il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e le modalità del trattamento di dati personali, nonché gli strumenti utilizzati, compreso il profilo della sicurezza.

b) RESPONSABILE DEL TRATTAMENTO

Può essere prevista, da parte del titolare, la nomina di uno o più responsabili del trattamento.
E' individuato tra i soggetti che per esperienza, capacità, affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.
I responsabili del trattamento, inoltre, hanno il compito di controllare, insieme agli amministratori di sistema, ognuno per le proprie specifiche competenze, l'efficacia di programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali e le misure minime di sicurezza.

Il Regolamento Europeo in materia di protezione dei dati personali fissa più dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti. Deve trattarsi di un vero e proprio contratto o atto giuridico (art.28 paragrafo 3) da adottarsi o da rivedersi con le necessarie modifiche o integrazioni.
Si prevedono inoltre obblighi specifici in capo ai responsabili poiché distinti da quelli pertinenti ai rispettivi titolari e riguardano in particolare la gestione delle misure tecniche e organizzative per garantire la sicurezza dei trattamenti adeguata ai rischi.

c) INCARICATO AL TRATTAMENTO

Gli incaricati sono le persone fisiche autorizzate dal titolare o dal responsabile a compiere operazioni di trattamento. Tali figure operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Gli incaricati devono essere designati individuando puntualmente l'ambito del trattamento consentito e nominati per iscritto dai responsabili delegati per la nomina dal titolare.

Pur non prevedendo espressamente la figura dell'incaricato del trattamento, il Regolamento Europeo non ne esclude la presenza parlando di esso come della 'persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile'.

d) L'INTERESSATO

È la persona fisica identificata o identificabile a cui si riferiscono i dati personali.
Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Tutti i diritti dell'interessato sono tutelati e garantiti dal Codice della Privacy e dal Regolamento Europeo.

e) DATA PROTECTION OFFICER (DPO)

Il Regolamento Europeo introduce per la prima volta la figura del Data Protection Officer (di seguito indicato come DPO) ovvero il Responsabile della Protezione Dati (RPD)
La nomina di questa figura riflette l'approccio responsabilizzante del Regolamento Europeo (art.39). Il compito principale è facilitare l'attuazione del regolamento stesso prevedendo anche la formazione al personale ovvero al titolare e ai responsabili del trattamento e la sorveglianza sullo svolgimento delle loro attività e la valutazione di impatto dei rischi.
La designazione è obbligatoria nel caso in cui il trattamento viene effettuato da un'autorità o da un organismo pubblico e nel caso in cui le attività di titolare e responsabili riguardano trattamenti che coinvolgono interessi su larga scala e categoria particolari di dati personali quali i dati sensibili, dati genetici, biometrici e giudiziari. La Pubblica Amministrazione deve quindi nominare obbligatoriamente il DPO.
È una figura che può essere designata anche esternamente all'Ente e deve avere necessariamente conoscenze e competenze sia in area giuridica (adeguata conoscenza della normativa privacy) che informatica (protezione dei dati tramite le misure minime di sicurezza finalizzate alla tutela) per valutare e disciplinare la gestione del trattamento e della salvaguardia dei dati personali.
Il Data Protection Officer deve:

- informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dallo stesso Regolamento Europeo e dalle evoluzioni normative
- sorvegliare l'applicazione e il rispetto del Regolamento Europeo nonché delle politiche programmate e adottate dal titolare e dal responsabile
- fornire consulenza normativa costante e pareri in merito alla valutazione d'impatto sulla protezione dei dati
- cooperare con l'Autorità garante fungendo da punto di contatto e intermediario per questioni connesse al trattamento

Per queste ragioni, il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e quindi riguardanti le misure tecniche in materia di sicurezza che si intendono adottare, sorvegliando sull'effettiva adozione.
Il DPO deve svolgere il proprio lavoro in completa autonomia, senza influenza da parte dell'Ente, anche qualora venga designato all'interno dell'Ente stesso. È una figura manageriale, di consulenza e di controllo.

Si consegna, contestualmente al presente documento, il testo delle 'Linee-guida sui responsabili della protezione dei dati', ovvero i DPO, nella versione emendata e adottata in data 5 aprile 2017. Queste linee guida forniscono le indicazioni necessarie per l'individuazione e la nomina del DPO e ne specifica il ruolo e i compiti.

f) INCARICATO DELLA MANUTENZIONE DEL SISTEMA

La figura non è espressamente prevista dal Codice della Privacy né dal Regolamento Europeo ma, nel caso specifico, si rende necessaria poiché il Comune non ha una completa autonomia gestionale dei sistemi informatici e dell'hardware installato e deve quindi ricorrere a imprese private esterne con le quali viene creato un rapporto fiduciario.
Il responsabile del trattamento, nello svolgimento delle sue funzioni istituzionali, vigila sulla correttezza di tale rapporto e sulle attività svolte dalle imprese esterne.
È necessario provvedere all'identificazione fisica degli incaricati della manutenzione e a farli sottoscrivere una lettera di impegno al rispetto della segretezza dei dati trattati.

LE FIGURE RILEVANTI

D.Lgs. n. 179/2016 (art. 17)

a) UFFICIO DIRIGENZIALE GENERALE

L'Amministrazione deve affidare a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità. All'ufficio sono attribuiti diversi compiti tra cui l'indirizzo, la pianificazione, il coordinamento e il monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture.

b) RESPONSABILE DELL'UFFICIO DIRIGENZIALE GENERALE

Il Responsabile dell'Ufficio è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali, attua i compiti necessari per la transizione digitale e risponde direttamente all'organo di vertice politico.

c) DIFENSORE CIVICO PER IL DIGITALE

Individuato di norma tra i dirigenti di ruolo in servizio, il Difensore Civico per il digitale è in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può inviare segnalazioni e reclami relativi ad ogni presunta violazione del D.Lgs. n. 179/2016 e di ogni altra norma in materia di digitalizzazione ed innovazione.
È intermediario tra il cittadino e il Responsabile dell'Ufficio Dirigenziale Generale, gestendo e trasmettendo le segnalazioni ritenute corrette e invitando l'Ufficio a porre rimedio tempestivamente e comunque nel termine di 30 giorni.

ANALISI DEI RISCHI

I rischi per i dati trattati e conservati da una Pubblica Amministrazione sono di due tipi: distruzione, perdita, cancellazione e sottrazione di dati informatici e sottrazione, distruzione e perdita di dati in supporti cartacei, siano essi archiviati o meno.
In riferimento ai rischi che minacciano la sicurezza dei dati, l'Ente deve quindi adottare determinate misure di sicurezza al fine di perseguire obiettivi di:

- riservatezza: i dati devono essere accessibili solo alle persone autorizzate. Tale principio, quando applicato, è in grado di ridurre il rischio che persone non autorizzate possano accedere alle informazioni.

- integrità: i dati devono essere protetti e preservati da possibili modifiche e danneggiamenti. Tale principio, quando applicato, è in grado di ridurre il rischio che le informazioni siano non volutamente modificate o cancellate o colposamente perse o distrutte.
- disponibilità: i dati devono essere accessibili alle persone autorizzate. Tale principio, quando applicato, riduce il rischio di non poter accedere ai dati anche se autorizzati dall'amministratore del sistema o dal titolare del trattamento.

Per poter programmare efficacemente e realmente una politica di sicurezza, le disposizioni del Codice della Privacy (D.Lgs. 196/2003) e del Regolamento Europeo in materia di protezione dei dati personali (n. 679/2016) devono essere necessariamente integrate con la Direttiva del Presidente del Consiglio dei Ministri attuata dalle Misure minime di sicurezza ICT per le Pubbliche Amministrazioni emanate da AGID.

Le Misure Minime AGID vogliono infatti aumentare la sicurezza ICT tramite una serie di interventi che sono mirati a garantire proprio la riservatezza, l'integrità e la disponibilità dei dati nonché a prevenire i rischi legati al trattamento e alla conservazione degli stessi. Si richiede infatti di:

- gestire attivamente tutti i dispositivi hardware e tutti i software presenti sulla rete
- istituire, implementare e gestire la configurazione di sicurezza di laptop, server e workstation per evitare attacchi informatici
- acquisire, valutare e intraprendere continuamente azioni per individuare vulnerabilità, correggendole e minimizzando il rischio di attacchi informatici
- istituire e gestire processi atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi
- gestire processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione di dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni, non solo di quelle oggetto del Codice in materia di protezione dei dati personali.

A seguito di analisi svolta e in base alla realtà del Comune, il livello della Circolare AGID a cui fare riferimento è il "Minimo", sotto il quale nessuna amministrazione può scendere. I controlli in esso indicati devono ritenersi obbligatori e pertanto da adottarsi tempestivamente qualora risultassero mancanti, e comunque non più tardi del 31 dicembre 2017.

IL SISTEMA INFORMATICO COMUNALE
VALUTAZIONE DEL LIVELLO DI SICUREZZA

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	**1**	**1**	**M**	**Implementare un inventario delle risorse attive correlato a quello ABSC 1.4**	L'inventario è riportato in allegato al presente documento ed elenca i dispositivi informatici collegati in rete in modo permanente.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	L'inventario al punto 1.1.1 viene generato tramite l'applicazione Spiceworks
1	**3**	**1**	**M**	**Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.**	L'elenco di cui alla misura 1.1.1 è aggiornato. L'aggiornamento dell'elenco è a carico degli Amministratori di Sistema.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	**4**	**1**	**M**	**Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.**	Vedi punto 1.1.1.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati	

				dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	**1**	**1**	**M**	**Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.**	L'elenco è riportato in allegato al presente documento L'aggiornamento dell'elenco dei software è a carico degli Amministratori di Sistema. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (vedi 5.1.1)
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	**3**	**1**	**M**	**Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.**	Gli Amministratori di Sistema eseguono periodicamente la verifica del software installato su ciascun dispositivo e

					comparano il risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco viene segnalato agli Amministratori di Sistema, che provvedono affinché venga rimosso o, se valutato necessario, a che venga inserito nell'elenco.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	L'inventario viene aggiornato con cadenza almeno annuale e ad avviene tramite l'utilizzo dell'applicazione Spiceworks.
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	**1**	**1**	**M**	**Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.**	La procedura prevede che ciascun sistema operativo, prima di essere messo in servizio, sia aggiornato con le patch più recenti e sia dotato di software antivirus e che gli account locali predefiniti siano protetti da password.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening	

				comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	**2**	**1**	**M**	**Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.**	Vedi 3.1.1.
3	**2**	**2**	**M**	**Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.**	Sono state date disposizioni agli amministratori di sistema in tale senso.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	**3**	**1**	**M**	**Le immagini d'installazione devono essere memorizzate offline.**	Le immagini di installazione dei sistemi operativi server sono su supporto DVD.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	.
3	**4**	**1**	**M**	**Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).**	Per attività di gestione effettuate da reti esterne alla rete comunale vengono utilizzati software commerciali (es. Teamviewer) che prevedono la cifratura delle informazioni.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	

3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	**1**	**1**	**M**	**Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.**	È stato installato un software specifico per la ricerca delle vulnerabilità. L'amministratore di rete provvede ad eseguire una scansione a fronte di una significativa modifica (installazione di un sistema o software nuovo, aggiornamento, modifica della configurazione) di uno o più sistemi o software.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di	

				vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	**4**	**1**	**M**	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**	L'amministratore di sistema provvede all'aggiornamento del software prima di ogni scansione.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	Sui sistemi operativi client vengono attivati gli aggiornamenti automatici per i sistemi operativi e gli applicativi che lo consentono. Sui sistemi operativi server gli aggiornamenti vengono scaricati e installati dall'amministratore di sistema con cadenza almeno semestrale.
4	**5**	**2**	**M**	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.**	Non sono presenti apparecchiature informatiche scollegate dalla rete.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	**7**	**1**	**M**	**Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.**	La risoluzione delle vulnerabilità è documentata dal report prodotto dal software di scansione.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	**8**	**1**	**M**	**Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).**	Si analizzano le azioni suggerite dal report prodotto dello strumento di scansione, agendo in base alle priorità ivi indicate.
4	**8**	**2**	**M**	**Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.**	Vedi 4.8.1 Sono state date disposizioni agli Amministratori di Sistema

4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	**1**	**1**	**M**	**Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.**	Le normali attività degli utenti richiedono la possibilità di aggiornare i software applicativi. Ciascun utente ha diritti amministrativi solo sul computer a lui assegnato.
5	**1**	**2**	**M**	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**	Gli eventi di accesso sono tracciati tramite i registri di Windows sul controllore di dominio.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	**2**	**1**	**M**	**Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.**	L'unica utenza amministrativa è l'utente "Administrator"
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	**3**	**1**	**M**	**Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	

5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	**7**	**1**	**M**	**Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	**7**	**3**	**M**	**Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	**7**	**4**	**M**	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	**10**	**1**	**M**	**Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.**	Gli utenti nominativi sono non privilegiati sulla rete. L'unica utenza privilegiata è l'amministratore di dominio. Tale utenza è utilizzata sotto la supervisione del personale autorizzato del comune.
5	**10**	**2**	**M**	**Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.**	Tutte le utenze sono nominative. Le credenziali dell'utenza amministrativa sono assegnate alla persona incaricata alla manutenzione dei sistemi. Tutte le operazioni vengono eseguite sotto la supervisione ed il controllo della persona incaricata.

5	**10**	**3**	**M**	**Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.**	L'architettura di rete di basa sull'utenza "Administrator" e non piò essere modificata.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	**11**	**1**	**M**	**Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.**	Le credenziali dell'utente Administrator sono in possesso della persona autorizzata e conservate in un documento apposito.
5	**11**	**2**	**M**	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	**1**	**1**	**M**	**Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.**	Su tutti i PC è installato un antivirus con aggiornamento automatico.
8	**1**	**2**	**M**	**Installare su tutti i dispositivi firewall ed IPS personali.**	Sui sistemi server è attivato Windows Firewall.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente	

				verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	**3**	**1**	**M**	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**	Al personale è stata fornita copia del regolamento interno per l'installazione e l'utilizzo dei sistemi informatici.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	**7**	**1**	**M**	**Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.**	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**2**	**M**	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**3**	**M**	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**4**	**M**	**Disattivare l'anteprima automatica dei contenuti dei file.**	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**8**	**1**	**M**	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**9**	**1**	**M**	**Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.**	Il sistema di posta elettronica è configurato in tal senso.

8	**9**	**2**	**M**	**Filtrare il contenuto del traffico web.**	Viene utilizzato il sistema di filtraggio del firewall.
8	**9**	**3**	**M**	**Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).**	Sono state date disposizioni agli amministratori di sistema di configurare il software antivirus delle postazioni di lavoro in tal senso.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	**1**	**1**	**M**	**Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.**	I servizi sono erogati da server fisico. Il backup dell'immagine del server viene effettuato ogni giorno su supporto USB removibile.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	**3**	**1**	**M**	**Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.**	Il sistema di backup utilizzato non prevede la cifratura. L'adeguamento avverrà in occasione della sostituzione dei server di rete. (Windows Server Backup)
10	**4**	**1**	**M**	**Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.**	In sistema di backup utilizzato non rende visibili le copie di backup dal lato utente. (Windows Server Backup)

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	**1**	**1**	**M**	**Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica**	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL).
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	**8**	**1**	**M**	**Bloccare il traffico da e verso url presenti in una blacklist.**	Vedi misura 8.9.2
13	9	1	A	Assicurare che la copia di un file fatta in	

				modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

Si consiglia di **aggiornare il presente documento nella sua parte riguardante la privacy** inserendo l'indicazione delle nomine e allegando copia degli atti, individuando ruoli e precise funzioni e responsabilità, applicando le necessarie modifiche o integrazioni alle attuali nomine di titolare e responsabile del trattamento, entro maggio 2018, quando il Regolamento Europeo entrerà in vigore, per la completa applicazione dello stesso.
A riguardo, si danno indicazioni per la nomina del DPO consegnando le linee guida che possono fornire supporto e chiarimenti per la scelta dello stesso e l'individuazione dei suoi compiti specifici.

Si raccomanda **l'individuazione e la nomina delle figure indicate** dall'articolo 17 del D.Lgs. 179/2016, poiché il Codice dell'Amministrazione Digitale è in vigore dal 14 settembre 2016 e di conseguenza queste figure sono da intendersi obbligatorie.
Non appena individuate, si raccomanda di allegare la nomina al presente documento.

È necessario provvedere all'**identificazione fisica degli incaricati della manutenzione del sistema comunale** e far sottoscrivere una lettera di impegno al rispetto della segretezza dei dati trattati, ove non già previsto nel contratto di manutenzione e assistenza.

Stante la situazione emersa in fase di indagine, si ritiene utile organizzare un corso di aggiornamento per formare il personale sulle modalità di transizione al digitale e di trattamento dei dati alla luce delle disposizioni normative in essere e degli aggiornamenti previsti per i prossimi mesi.
Tutto il personale deve infatti essere costantemente informato e formato sulle procedure da seguire e sui comportamenti corretti da attuare, sui rischi che si corrono e sulla prevenzione degli stessi.

ANALISI DELLA SITUAZIONE COMUNALE: problematiche generali

a) Aspetti logistici e trattamento dati in formato elettronico: strumenti e dotazioni informatiche

.

Tutte le postazioni di lavoro sono protette da password che si consiglia non conservare in formato cartaceo nei pressi della postazione stessa, né salvare sul pc stesso, né comunicare a terzi, salvo al responsabile del trattamento, se previsto dalla nomina, o ad altri incaricati del trattamento. Anche l'accesso ai programmi gestionali è protetto da password, per il quale si raccomandano le stesse indicazioni.

È necessario inoltre che l'incaricato non lasci mai incustodita la propria postazione di lavoro con programmi e documenti aperti. In caso di allontanamento è necessario che dopo un breve periodo si attivi uno screen saver che oscuri la schermata e che richieda l'inserimento della password alla ripresa dell'attività lavorativa.

b) Aspetti logistici e trattamento dati in formato non elettronico: strumenti e dotazioni

I rischi per i dati conservati in formato cartaceo riguardano la perdita accidentale o deliberata, la distruzione, eventi naturali dolosi o colposi come incendio e allagamento, il furto e gli accessi abusivi agli archivi di conservazione dei dati.

Per garantire la sicurezza dei locali comunali è necessario che l'edificio sia dotato di idonei sistemi di allarme e tutte le porte e le finestre siano munite di sistemi antintrusione.

Gli uffici e gli arredi devono essere mantenuti chiusi e non accessibili al pubblico e/o a persone non autorizzate. Per questo, è necessario che ciascun ufficio organizzi la chiusura a chiave degli stessi e la gestione delle chiavi.

Inoltre, in loro assenza, si consiglia di mantenere sempre chiusi a chiave l'ufficio del Sindaco e del Segretario Comunale.

Per quanto concerne armadi e cassettiere, pur non essendo di tipo ignifugo e blindati, la dotazione degli uffici appare sufficientemente sicura se adottati i provvedimenti di cui al punto precedente.

L'archivio dovrebbe essere sempre chiuso a chiave e la custodia delle stesse affidata al responsabile del trattamento dei dati. Dovrebbe inoltre essere predisposta una circolare interna che regoli l'utilizzo dell'archivio generale e predisposto un registro che riporti l'accesso all'archivio generale e soprattutto la movimentazione dei documenti, che comunque non possono uscire dalla struttura comunale per nessuna ragione, salvo particolari accordi appositamente autorizzati.

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI

I modelli che si consegnano congiuntamente al presente documento sono:

1) *CIRCOLARE G.U. 18 aprile 2017 n. 2/2017*
2) *ALLEGATO A - ANALISI DEI RISCHI*
3) *ALLEGATO B – LINEE GUIDA SUI RESPONSABILI DELLA PROTEZIONE DEI DATI*
4) *ALLEGATO C – INVENTARIO DISPOSITIVI*
5) *ALLEGATO D - INVENTARIO SOFTWARE*
6) *ALLEGATO E – REGOLAMENTO INFORMATICO*

MODALITA' DI AGGIORNAMENTO

Il documento deve essere aggiornato ogni volta che vi sono cambiamenti significativi nella struttura dell'Ente impattanti sulle misure minime di sicurezza e rispetto ai ruoli assegnati ovvero in caso di nuove e diverse indicazioni normative e disposizioni di legge.
In ogni caso, si consiglia di procedere alla revisione del documento in oggetto con scadenza annuale.

Al documento, prima della revisione annuale, devono essere necessariamente allegati:

- copia degli atti con cui si provvede alla nomina delle figure rilevanti (pag.5-8)
- copia del modulo di implementazione richiesto da AGID (pag.11), compilato e riportante le indicazioni sull'attuale stato del sistema ICT e su come è intenzione agire per adeguare e implementare tutto ciò che invece risulta mancante o inadeguato.

Vilanova Monferrato, 02/02/2018