COMUNE DI MARANO SUL PANARO
Provincia di Modena

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 98 del 20/12/2017

OGGETTO: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI.

L'anno **duemiladiciassette** addì **venti** del mese di **dicembre** alle ore **18:30** nella Casa Comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente legge comunale e provinciale, vennero oggi convocati a seduta i componenti la Giunta Comunale, che nelle persone seguenti risultano presenti alla trattazione della proposta di deliberazione in oggetto:

MURATORI EMILIA	SINDACO	Presente
GALLI GIOVANNI	VICE SINDACO	Presente
RONDELLI MAURO	ASSESSORE	Presente
DANI ELIO	ASSESSORE	Presente
ZANANTONI RITA	ASSESSORE	Presente

Presenti n. 5 **Assenti n. 0**

Partecipa il SEGRETARIO COMUNALE MARTINI MARGHERITA che provvede alla redazione del presente verbale.

Presiede la seduta, nella sua qualità di SINDACO, il Sig. MURATORI EMILIA che dichiara aperta la trattazione dell'oggetto sopra indicato.

Deliberazione n. 98 del 20/12/2017

OGGETTO: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI.

LA GIUNTA COMUNALE

PREMESSO

- che il Codice dell'amministrazione digitale (CAD) di cui al D. Lgs. n.82/2005, come aggiornato dal D. Lgs. n. 179/2016, attuativo dell'art.1 della Legge n.124/2015 di riforma della Pubblica Amministrazione, è entrato in vigore il 14/09/2016 e impone a tutte le P.A. di nominare un unico Ufficio dirigenziale generale responsabile per la transizione al digitale;
- che al responsabile competono tutte le attività operative finalizzate alla transizione e i conseguenti
processi di riorganizzazione funzionali alla realizzazione di un'amministrazione digitale aperta all'erogazione di servizi facilmente utilizzabili e di qualità, nonchè al raggiungimento di migliori standard di efficienza ed economicità;
- che il responsabile ha poteri di impulso e coordina mento e deve assicurare il rispetto degli obblighi
previsti dalla normativa vigente (Codice dell'Amministrazione digitale e relative regole attuative, Piano
triennale per l'informatica nella P.A., ecc...);

CONSIDERATO

- che il processo di riforma, come avviato, pone in capo ad ogni Amministrazione la necessità di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione, centralizzando in capo ad un ufficio unico il compito di accompagnare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione, con l'obiettivo generale di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
- che, a norma dell'art.17 del CAD ("Strutture per l'organizzazione, l'innovazione e le tecnologie"), l'ufficio dirigenziale generale responsabile della transizione al digitale, ha i seguenti compiti:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge n.4 del 09/01/2004;
e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché' di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione
dei sistemi informativi di telecomunicazione e fonia;
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio

dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e man-dato informatico, e delle norme in materia di accessibilità e fruibilità;
- che il Responsabile dell'ufficio per la transizione digitale deve essere trasversale a tutta l'organizzazione;
- che il Responsabile dell'ufficio per la transizione digitale deve essere dotato di adeguate competenze
tecnologiche;
RILEVATO CHE la Dott.ssa Elisabetta Manzini essendo Responsabile del Settore Affari Generali è l'unico Funzionario ad avere un ruolo trasversale a tutta l'organizzazione ed è sufficientemente dotata di conoscenze tecnologiche;
DATO ATTO che i processi e i procedimenti necessitano di una adeguata analisi e successivo adeguamento rispetto a quanto stabilito dalla normativa vigente, alla luce anche delle recenti modifiche intervenute in materia di pubblicità e trasparenza di cui al D. Lgs.n. 33/2013, come revisionato a seguito dell'entrata in vigore del D. Lgs. n. 97/2016 (Freedom of Information Act - FOIA);
DATO ATTO inoltre che i sistemi informatici in uso nel Comune dovranno essere modificati ed allineati a quanto risulterà dall'analisi dei processi;
RICHIAMATA la Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale;
PRESO ATTO di quanto disposto dall'AGID la quale ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".
CONSIDERATO che l'adeguamento delle Pubbliche amministrazioni alle Misure minime dovrà avvenire entro il **31 dicembre 2017,** a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, del dirigente allo scopo designato.
RITENUTO di provvedere a nominare il Responsabile della transizione alla modalità operativa digitale nella persona della Dott.ssa Elisabetta Manzini;
RITENUTO inoltre di provvedere a prendere atto del documento contemplante l'elenco delle "Misure minime per la sicurezza ICT delle pubbliche Amministrazioni" predisposto dal Servizio Ced dell'Unione Terre di Castelli ed allegato al presente atto quale parte integrante e sostanziale;
DATO ATTO che il suddetto Responsabile nominato con il presente atto provvederà a siglare digitalmente il documento di cui al punto precedente;
V
VISTO lo Statuto Comunale;
VISTO il D.Lgs.vo 18 agosto 2000, n. 267 e successive modificazioni ed integrazioni;
DATO ATTO che ai sensi dell'art. 49 del citato D.Lgs n.267/2000, sulla proposta della presente deliberazione ha espresso parere favorevole il responsabile del servizio interessato, dott.ssa Elisabetta Manzini, in ordine alla sola regolarità tecnica;
DATO ATTO altresì che il presente provvedimento non comporta alcuna spesa a carico del bilancio del corrente esercizio;
Con voti favorevoli unanimi, espressi per alzata di mano ed accertati nei modi e nelle forme di legge,

DELIBERA

1. Di nominare, per le ragioni di cui in premessa, della transizione alla modalità operativa digitale nella persona della Dott.ssa Elisabetta Manzini;
2. Di prendere atto dei contenuti dell'elenco delle "Misure minime per la sicurezza ICT delle pubbliche Amministrazioni" predisposto dal Servizio Cede dell'Unione Terre di Castelli ed allegato al presente atto quale parte integrante e sostanziale (ALLEGATO A);
3. Di dare atto che il Responsabile nominato al punto 1), provvederà a siglare digitalmente il documento di cui al precedente punto 2);

SUCCESSIVAMENTE

Stante l'urgenza di provvedere in merito,

LA GIUNTA COMUNALE

Con voti favorevoli unanimi, espressi per alzata di mano ed accertati nei modi e nelle forme di legge,

DELIBERA

altresì di dichiarare il presente atto immediatamente eseguibile, ai sensi e per gli effetti di cui al comma 4 dell'art. 134, del D. Lgs.vo n. 267 del 18/8/2000

COMUNE DI MARANO SUL PANARO
Provincia di Modena

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL SINDACO	IL SEGRETARIO COMUNALE
MURATORI EMILIA	MARTINI MARGHERITA

Comune di Marano sul Panaro

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 delle risorse è disponibile all'URL https://web1.terredicastelli.mo.it/inventario. L'accesso è protetto e monitorato dal firewall Sophos UTM 9, inoltre è necessario disporre di una coppia username/password che consente l'accesso solo al personale del servizio Sistemi informativi dell'Unione Terre di Castelli.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Il servizio DHCP è in fase di dismissione.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'inventario (vedi punto 1.1.1) viene mantenuto aggiornato manualmente dal servizio Sistemi informativi dell'Unione Terre di Castelli quando un nuovo dispositivo approvato (postazione, stampante di rete, apparato di rete) è installato.
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.	Nell'inventario (vedi punto 1.1.1) è sempre registrato anche l'indirizzo IP del dispositivo.
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.	Nell'inventario (vedi punto 1.1.1) sono sempre registrati il nome del dispositivo e la tipologia (switch, portatile, PC, stampante di rete, ecc…). Viene inoltre registrata la collocazione (ente di

				L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	appartenenza, collocazione sede e ufficio) e il nominativo dell'utilizzatore o degli utilizzatori.
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 di software autorizzati verrà realizzato entro il 31/01/2017 e sarà disponibile in formato PDF all'interno della intranet dei Comuni e dell'Unione nella sezione Regolamenti (URL: http://intra.uni.priv/?q=node/23), in quanto ritenuto parte integrante del regolamento di utilizzo delle postazioni. L'elenco sarà aggiornato periodicamente dall'ufficio Sistemi Informativi dell'Unione Terre di Castelli.
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.	La scansione del software viene effettuata manualmente dal personale dei servizio Sistemi informativi dell'Unione Terre di Castelli ogni volta che si rende necessaria la manutenzione di una postazione di lavoro.
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.	
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 configurazione di base dei sistemi operativi consiste nell'applicazione di group policy di dominio che impostano le caratteristiche generali per tutti gli utenti (proxy, siti attendibili, impostazioni screen saver e blocco postazione). L'antivirus è centralizzato su server. Le patch dei sistemi operativi sono distribuite attraverso WSUS, con regolare controllo delle anomalie. E' inoltre in uso un firewall centralizzato per il blocco di porte e servizi non autorizzati.

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.	Le configurazioni standard delle postazioni sono gestite (quando le postazioni installano sistema operativo Microsoft Windows) tramite distribuzione WDS. L'immagine WDS esiste per le postazioni acquistate a partire dal 2015, per le postazioni meno recenti non si ritiene conveniente acquisire una immagine dedicata, in quanto la tendenza è quella di sostituirle con postazioni più recenti. Le configurazioni di sicurezza delle postazioni sono propagate mediante group policy di dominio, il login e l'accesso alle risorse di rete sono gestiti da script. Su ogni postazione è installato l'antivirus centralizzato. I server sono gestiti tramite ova e template.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	La postazione compromessa è ritirata e reinstallata con l'immagine WDS corrispondente, che la ripristina alla configurazione standard. Se la postazione non possiede una immagine di ripristino (quindi è datata) si provvede alla sostituzione.
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.	Una copia delle immagini WDS, i template e gli ova sono salvati su un disco offline.
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).	L'amministrazione dei dispositivi di rete è permessa solo da alcune postazioni autorizzate e su una vlan dedicata e non accessibile dall'esterno. I server sono accessibili in RDP e da console VMWare solo dalle postazioni dei sistemi informativi. Le postazioni di lavoro sono raggiunte, per l'assistenza remota, tramite Teamviewer Quick Start (non installato residente sulle macchine, ma scaricato e avviato solo in caso di necessità.
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.	L'organizzazione ha investito molto sulla protezione perimetrale e sulla configurazione ottimale delle LAN, infatti non è attivo nessun servizio DHCP, non sono disponibili punti di accesso wi-fi collegati alle reti locali e non è possibile procedere alla navigazione senza impostare il proxy con relativo web filtering. Inoltre le patch dei sistemi operativi sono distribuite tramite WSUS a tutti i dispositivi e l'antivirus viene mantenuto costantemente aggiornato. Pertanto non disponiamo di un sistema di ricerca delle vulnerabilità automatizzato, vengono tuttavia svolti dei controlli periodici attraverso la consultazione dei log e degli alert del firewall e del server antivirus. Inoltre viene controllato lo stato di aggiornamento dei client e dei server attraverso la reportistica di WSUS. I server sono aggiornati sia attraverso WSUS che attraverso un controllo e aggiornamento mensile manuale. I firewall sono aggiornati costantemente ogni volta che sono disponibili nuove patch o firmware.
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.	Gli strumenti di cui al punto 4.1.1 sono costantemente aggiornati non appena disponibili nuove patch o firmware.
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.	I sistemi operativi Windows sono aggiornati automaticamente tramite WSUS, per quanto riguarda i sistemi Unix/Linux (utilizzati esclusivamente per i server) non si ritiene operativamente conveniente adottare tecniche di aggiornamento automatico, in quanto aggiornamenti e patch possono pregiudicare il corretto funzionamento degli applicativi sopra installati, con conseguente danno operativo ed economico, in caso di ripristino da parte del fornitore. Lo stesso ragionamento è valido per le applicazioni o i componenti necessari al loro funzionamento (ad esempio java VM), in quanto gli aggiornamenti richiedono una preventiva fase di testing da parte del servizio sistemi informativi prima di poter essere distribuiti in produzione.
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 dispositivi che rientrano in queste categorie.
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 correzione delle vulnerabilità, come detto al punto 4.1.1, è svolta nelle modalità descritte per quanto concerne la parte di installazione sui dispositivi di patch e firmware, mentre per la gestione delle anomalie impreviste si interviene a fronte di un alert da parte di antivirus o firewall, anche isolando dalla rete l'elemento che presenta un comportamento anomalo.
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.).	Il piano di gestione è in fase di definizione, sarà ultimato entro il 31 marzo 2018.
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 punto 4.8.1
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	Occorre distinguere i privilegi di amministrazione in due categorie, che hanno impatti e funzionalità decisamente differenti.

				la configurazione dei sistemi.	1: amministratore di server e dispositivi, figura associata al personale del servizio Sistemi Informativi e ai fornitori di servizi. 2: amministratore locale della postazione di lavoro. Gli amministratori al punto 1 sono ben identificati, i server sono monitorati da un syslog centralizzato. Gli amministratori locali della postazione di lavoro coincidono invece con gli utenti della postazione stessa, in quanto non è pensabile limitarne i privilegi, poiché i software di produttività non sono in grado di funzionare correttamente e le versioni più recenti di Windows sono troppo limitative per consentire agli operatori di svolgere anche la più banale attività. In termini di costi/benefici gli enti subirebbero un danno economico decisamente maggiore cercando continuamente di gestire un funzionamento accettabile di macchine con accesso limitato, valutando le diverse casistiche d'uso, piuttosto che accettare che una postazione di lavoro, saltuariamente, possa essere compromessa, visto anche che i tempi di ripristino della stessa sono piuttosto rapidi. Alcune limitazioni di massima sono comunque imposte da group policy di dominio, pertanto gli utenti non hanno la completa autonomia sulla gestione delle postazioni.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Come detto al punto 5.1.1 i server sono monitorati sotto syslog, pertanto gli accessi sono registrati. Le utenze amministrative sono utilizzate solo per scopi di gestione, configurazione e manutenzione degli stessi. In caso di server con accesso ad utenti non IT (ad esempio i server terminal), gli utenti sono configurati con accesso limitato.
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.	Le utenze amministrative sono correntemente censite. L'unico personale dell'ente autorizzato ad accedere ai server e ai dispositivi di rete con un utenza amministrativa è quello del

					servizio Sistemi Informativi dell'Unione Terre di Castelli. Il sistema di autorizzazione è da revisionare, in particolare per quanto concerne la gestione degli accessi dei fornitori esterni, che necessitano, per lo svolgimento delle attività di manutenzione e assistenza, di un accesso amministrativo a determinate risorse.
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.	Questa operazione è svolta regolarmente.
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).	Come detto al punto 5.2.1, il sistema di gestione delle credenziali è in fase di revisione totale. E' un'attività legata a diversi fattori, su cui si sta cercando una soluzione di convergenza. La dimensione e l'eterogeneità della rete e del data center non consente una soluzione rapida al problema, in quanto non è completa l'unificazione dei domini dei vari enti e non si è potuto ancora implementare completamente un sistema unico di gestione delle credenziali. Il lavoro di unificazione di 98 server e circa 500 client è

					un onere molto gravoso per il servizio Sistemi Informativi servizio Sistemi informativi dell'Unione Terre di Castelli, che conta solo 4 unità tecniche che si occupano di un ventaglio di attività estremamente variegato: dall'help desk di primo livello alla gestione del data center e della rete geografica di tutto il territorio dell'Unione, senza avvalersi di ausili esterni per la manutenzione ordinaria delle postazioni. Ci sono inoltre da considerare le criticità legate al funzionamento operativo di alcuni applicativi che devono essere sanate (in primis dai fornitori) prima che si possa intervenire con la sostituzione a norma delle credenziali amministrative. E' in fase di redazione un regolamento per la somministrazione delle credenziali amministrative ai fornitori, dopodiché, compatibilmente con la disponibilità finanziaria, si provvederà ad implementare un sistema di gestione delle credenziali di livello avanzato.
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).	Vedi punto 5.7.1
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Vedi punto 5.7.1
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.	Vedi punto 5.7.1
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Vedi punto 5.7.1
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.	Vedi punto 5.7.1
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.	Una copia dell'elenco delle credenziali è conservata in una cassaforte ad accesso esclusivo del personale del servizio Sistemi Informativi dell'Unione Terre di Castelli.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non sono attualmente in uso certificati digitali per l'autenticazione.

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.	Attualmente tutte le postazioni sono dotate di antivirus TrendMicro OfficeScan, gestito centralmente e aggiornato in modo automatico quotidianamente. Il sistema, in caso di anomalie rilevanti, invia una mail al servizio sistemi informativi con l'identificazione della postazione e il report dei problemi trovati.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	
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.	Si, è già così.
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.	Sì, è già così.
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.	L'organizzazione non fa uso di dispositivi esterni per attività lavorative, fatta eccezione per la web mail, che comunque è monitorata e protetta dal firewall e dal mail filter.
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.	A fronte della redazione del nuovo regolamento d'uso delle postazioni informatiche sarà attivata una group policy di dominio che inibisce l'esecuzione automatica dei contenuti dei dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'esecuzione dei contenuti dinamici dei file è necessaria allo svolgimento dell'attività lavorativa, pertanto non si ritiene

					conveniente la disattivazione, ritenendo il rischio accettabile.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'anteprima dei messaggi di posta elettronica è gestita da una impostazione globale delle policy di Zimbra.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	A fronte della redazione del nuovo regolamento d'uso delle postazioni informatiche sarà attivata una group policy di dominio che inibisce l'anteprima automatica.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'antivirus è impostato per eseguire la scansione dei supporti rimovibili
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.	Per la posta elettronica aziendale è in uso la funzione mail filtering di Sophos, installata su due dispositivi in HA di tipo UTM9.
8	9	2	M	Filtrare il contenuto del traffico web.	Per tutte le postazioni di lavoro e i server è in uso la funzione web filtering di Sophos, installata su due dispositivi in HA di tipo UTM9.
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).	Per la posta elettronica aziendale è in uso la funzione mail filtering di Sophos, installata su due dispositivi in HA di tipo UTM9.
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.	Ogni giorno, a partire dalle ore 0:00 viene avviato il backup dell'intera infrastruttura virtuale verso un data center remoto (attualmente presso Lepida SPA). Il backup copia tutte le macchine virtuali del data center ed è effettuato con Veeam Backup Enterprise Edition. I punti di ripristino totali per ciascun server sono 7, ogni mese è svolto il controllo automatico dell'integrità del task

					e periodicamente vengono fatti dei test di ripristino da parte del personale del servizio Sistemi Informativi dell'Unione Terre di Castelli.
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.	Vedi punto 10.1.1
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 data center dell'Unione Terre di Castelli, che convoglia al suo interno i server dell'Unione e dei Comuni è composto da un'infrastruttura virtuale VMWare che conta 98 server in produzione e uno storage di 35 TB attivi. L'infrastruttura di backup è costituita da un server Veeam Backup con due ulteriori server che svolgono la funzione di proxy di backup. Lo storage di backup è esternalizzato sul data center di Lepida SPA e attualmente raggiunge i 25 TB di spazio occupato. Lo storage non è in alcun modo raggiungibile da altre reti se non dalla LAN del data center e non è visibile ai client. Data la sicurezza strutturale dell'infrastruttura e la mole di dati del backup è impensabile riuscire a garantire un backup giornaliero se ad esso si va a sommare l'onere di crittografare i dati (il tempo di esecuzione dei backup triplicherebbe, superando abbondantemente le 24 ore), in più ciò comporterebbe l'acquisto di risorse informatiche aggiuntive per il data center, cosa che attualmente non è permessa, né motivabile. Pertanto per gli enti non vi è nessun vantaggio nel ridurre la disponibilità di punti di ripristino per crittografare le copie.
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.	Come detto al punto 10.3.1 la grandezza delle copie non consente di utilizzare più punti di accesso. Si ritiene inoltre accettabile il rischio, in quanto sia il server Veeam che lo storage di backup non sono visibili dalla rete locale e non condividono risorse raggiungibili

					dai client.

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 dati deve essere svolta in funzione del nuovo censimento delle banche dati, dopo di che andrà individuato uno strumento adatto alle operazioni di crittografia che sarà acquistato e implementato se le risorse finanziarie lo consentono.
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.	Il controllo del traffico avviene attraverso il firewall Sophos, installato su due dispositivi in HA di tipo UTM9.
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.	

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Proposta N. 2017 / 1379
UNITA' PROPONENTE Amministrativo

OGGETTO: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI.

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Per i fini previsti dall'art. 49 del D. Lgs 18.08.2000 n° 267, si esprime sulla proposta di deliberazione in oggetto parere *FAVOREVOLE* in merito alla regolarità tecnica.

Marano sul Panaro, 19/12/2017

IL RESPONSABILE DI SETTORE
MANZINI ELISABETTA
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Proposta N. 2017 / 1379
UNITA' PROPONENTE Amministrativo

OGGETTO: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI.

PARERE IN ORDINE ALLA REGOLARITA' CONTABILE

Il sottoscritto, in qualità di Responsabile del Settore Economico Finanziario, ai sensi dell'art. 49, comma 1 e dell'art. 147-bis, comma 1, D.Lgs 267/2000, esprime sulla proposta di deliberazione in oggetto parere NON APPOSTO in merito alla regolarità contabile.

Marano sul Panaro, 19/12/2017

IL RESPONSABILE DI SETTORE
ZANNI PATRIZIA
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Certificato di Pubblicazione

Deliberazione di Giunta Comunale N. 98 del 20/12/2017

Amministrativo

Oggetto: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI..

Ai sensi per gli effetti di cui all'art. 124 del D.Lgs 18.8.2000, n. 267 copia della presente deliberazione viene pubblicata, mediante affissione all'Albo Pretorio, per 15 giorni consecutivi dal 08/01/2018.

Marano sul Panaro, 08/01/2018

L'INCARICATO DELLA PUBBLICAZIONE
MARTINI MARGHERITA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Certificato di Esecutività

Deliberazione di Giunta Comunale N. 98 del 20/12/2017

Amministrativo

Oggetto: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI..

Si dichiara che la presente deliberazione è divenuta esecutiva decorsi 10 giorni dall'inizio della pubblicazione all'Albo Pretorio on-line di questo Comune.

Marano sul Panaro, 22/01/2018

L'INCARICATO DELLA PUBBLICAZIONE
MARTINI MARGHERITA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Certificato di Avvenuta Pubblicazione

Deliberazione di Giunta Comunale N. 98 del 20/12/2017

Oggetto: NOMINA DELL'UFFICIO DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITA' OPERATIVA DIGITALE ED ADOZIONE MISURE MINIME PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI. PROVVEDIMENTI..

Si dichiara l'avvenuta regolare pubblicazione della presente deliberazione all'Albo Pretorio on-line di questo Comune a partire dal 08/01/2018 per 15 giorni consecutivi, ai sensi dell'art 124 del D.lgs 18.08.2000, n. 267 e la contestuale comunicazione ai capigruppo consiliari ai sensi dell'art. 125 del D.lgs 18.08.2000, n. 267.

Marano sul Panaro, 24/01/2018

L'INCARICATO DELLA PUBBLICAZIONE
MARTINI MARGHERITA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)