COMUNE DI BUSSETO

Provincia di Parma

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N. ATTO 207 ANNO 2017

SEDUTA DEL 28/12/2017 ORE 15:00

OGGETTO: PIANO DELLE MISURE MINIME DI SICUREZZA INFROMATICA – ADOZIONE.

L'anno duemiladiciassette il giorno ventotto del mese di Dicembre alle ore 15:00 nella sede comunale, previo esaurimento delle formalità prescritte dalla Legge e dallo Statuto, si è riunita sotto la presidenza del Sindaco Giancarlo Contini, la Giunta Comunale.

All'Appello Risultano

ASSESSORI	PRESENTI	ASSENTI
CONTINI GIANCARLO	PRESENTE	
LEONI GIANARTURO	PRESENTE	
CAPELLI STEFANO	PRESENTE	
GUARESCHI ELISA		ASSENTE
MARCHESI MARZIA		ASSENTE

Totale presenti: n. 3
Totale assenti : n. 2

Partecipa all'adunanza Il Vice Segretario Stellati Dott.ssa Elena, il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti Il Sindaco Giancarlo Contini assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopraindicato

COMUNE DI BUSSETO

Provincia di Parma

OGGETTO: PIANO DELLE MISURE MINIME DI SICUREZZA INFROMATICA – ADOZIONE.

LA GIUNTA COMUNALE

VISTA la direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che prevede l'emanazione di provvedimenti con cui l'Agenzia per l'Italia Digitale impartirà disposizioni sugli adempimenti tecnologici ed organizzativi a cui le pubbliche amministrazioni dovranno adeguarsi al fine di contrastare eventuali attacchi cibernetici allineandosi a quanto previsto dagli standard di sicurezza classificati come "minimi";

VISTA la circolare AGID 18 aprile 2017 n. 2/2017 "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: <<Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)>> con cui si stabilisce l'obbligo di adeguamento per le Amministrazioni individuate nell'art. 2 c. 2 del CAD;

ATTESO che la scadenza per l'adeguamento è fissata al 31/12/2017 e l'adempimento è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie come definito dall'art. 17 del CAD o in sua assenza, in alternativa, del dirigente allo scopo designato;

RILEVATO che le misure di adeguamento consistono in una serie di adempimenti tecnico-organizzativi dettagliati nell'allegato 1 alla circolare AGID 2/2017 e che le pubbliche amministrazioni devono adeguarsi alle misure classificate come MINIME e dettagliate nell'allegato 2 allo stesso provvedimento;

VISTO che il dirigente designato all'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla circolare;

VISTE le proposte di misure di protezione elaborate dalla ditta POLARIS per conto del Comune di Busseto con la collaborazione del Settore Affari Generali e Servizi Istituzionali preposto al fine di adeguarsi agli standard classificati come "minimi";

RITENUTO di approvarle;

ACQUISITO il parere favorevole reso dal Responsabile dell'Ufficio Affari Generali in ordine alla regolarità tecnica, ai sensi dell'art. 49, comma 1 del D. Lgs.vo n. 267/2000 e s.m., da ultimo modificato dall'art. 3.1 lett. d), del D.L. n. 174/2012;

OMESSO il parere favorevole reso dal Responsabile di Ragioneria in ordine alla regolarità contabile non implicando la proposta gli effetti cui la norma lo subordina;

CON VOTI unanimi favorevoli resi in forma palese ai sensi di legge,

DELIBERA

1) DI APPROVARE le misure minime di sicurezza ICT per il Comune di Busseto come dettagliate nell'allegato documento;

Successivamente,

LA GIUNTA COMUNALE

ravvisata l'urgenza di provvedere in merito, con separata votazione, con voti unanimi favorevoli resi in forma palese ai sensi di legge,

DELIBERA

di dichiarare il presente atto immediatamente eseguibile ai sensi dell'art. 134.4 del D.lgs.vo n° 267/2000 e s.m.

Il presente verbale viene letto e sottoscritto come segue.

Il Sindaco	Il Vice Segretario
Giancarlo Contini	Stellati Dott.ssa Elena

COMUNE DI BUSSETO

Provincia di Parma

VISTO DI REGOLARITA' TECNICA
(art 49 comma 1 del T.U.E.L. D.Lgs 267/2000)

Proposta di delibera di Giunta avente per oggetto:

Piano misure minime di sicurezza informatica – Adozione.

Il sottoscritto, responsabile di servizio esprime **parere favorevole** in ordine alla regolarità tecnica della proposta di deliberazione in oggetto, precisando che sono state osservate le procedure preliminari di legge e dei regolamenti.

Busseto, lì 28/12/2017

Responsabile area affari
generali e Servizi Istituzionali
SORENTI MERENDI ALVI
GIANCARLO / Poste Italiane
S.p.A.

COMUNE DI BUSSETO

Provincia di Parma

Deliberazione di Giunta Comunale
N. 207
DEL 28/12/2017
OGGETTO: PIANO DELLE MISURE MINIME DI SICUREZZA INFROMATICA – ADOZIONE.

RELATA DI PUBBLICAZIONE

Il sottoscritto

visti gli atti d'ufficio

ATTESTA

Che la presente deliberazione:

- viene pubblicata nell'Albo On Line di questo Comune per 15 giorni consecutivi dal 02/01/2018 al 17/01/2018

Busseto lì 02/01/2018

L' addetto

Stefania Macchidani / INFOCERT SPA

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione	
1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario dei dispositivi è disponibile sul portale https://utv.polaris.it
1	1	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'inventario viene aggiornato con l'aggiunta di nuovi dispositivi e nuovi utenti, sempre sul portale https://utv.polaris.it

1	3	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	L’inventario viene gestito tramite il portale https://utv.polaris.it
1	4	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	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	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	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.	Elenco presente sul server del comune, dentro la cartella “Dati\Polaris\Misure Sicurezza ICT”. Il documento si chiama ELENCO SOFTWARE AUTORIZZATI.
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 viene effettuata da un software, che controlla a intervalli regolari la presenza di software non autorizzati in rete. Regolarmente il software invia dei Report all'amministratore di rete.
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	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Vengono utilizzate le configurazioni standard dell'ambiente Microsoft Windows, con la presenza di un dominio, utenze di dominio protette da password e cartelle di rete con accessi protetti da password.

3	1	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	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	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	L'ambiente deciso per il comune basato su software Windows, segue uno standard per ogni Client. Tutti gli utenti utilizzano lo stesso sistema

				operativo, stesso sistema di posta elettronica, etc… Alla rottura di una workstation, l'utente può utilizzare una nuova postazione utilizzano le sue credenziali di dominio.
3	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Questa è la procedura standard, adottata dal comune. Alla rottura di una postazione, a seconda della disponibilità, l'utente può utilizzare una nuova postazione semplicemente utilizzano le sue credenziali di dominio e dei vari sistemi presenti.
3	2	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	M	Le immagini d'installazione devono essere memorizzate offline.	Dovuto alla grande diversità delle postazioni utenti, non è presente una immagine installazione.
3	3	S	Le immagini d'installazione sono conservate in modalità	

			protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	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).	Le operazione da remoto vengono eseguite tramite software protetto da criptografia (Teamviewer o VPN SSL).
3	5	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	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	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	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	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	M	Ad ogni modifica	Sia il Server che i

			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.	dispositivi di rete sono monitorati quotidianamente, un sistema con vari tipi di Alert è predisposto e alla presenza di errori o possibile falle di sicurezza una mail viene inviata all'amministratore di rete.
4	1	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	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	S	Correlare i log di sistema	

			con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	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	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	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano	Gli strumenti sono sempre aggiornati all'ultima versione fornita dai rispettivi

			regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	produttori.
4	4	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti del Server e delle applicazioni sono impostati sempre su automatico dove possibile. I software che non hanno un sistema di aggiornamento automatico, vengono aggiornati a seconda della disponibilità fornita dai produttori.
4	5	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Il comune di Busseto è in regola.
4	6	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	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.	Gli aggiornamenti del Server e delle applicazioni sono impostati sempre su automatico dove possibile. I software che non hanno un sistema di aggiornamento automatico, vengono aggiornati a seconda della disponibilità fornita dai produttori.
4	7	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	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e	Il piano di gestione dei rischi è mantenere tutti i sistemi aggiornati, limitare al massimo l'uso di sistemi obsoleti o non più coperti da supporto,

			della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	tenere i dati importanti e sensibili dove viene fatto un backup giornaliero, limitare l'accesso alla rete e ai dispositivi. Si tiene conto che tutti i sistemi sono possibilmente esposti a rischi, anche quelli aggiornati, e quindi per il comune si è scelto di optare per la sicurezza dei dati tramite backup.
4	8	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.	Le azioni sono quelle di aggiornare sempre se possibile, le patch vengono applicate appena rese disponibili dai produttori.
4	9	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	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		Solamente i tecnici hanno diritti amministrativi dove ci sono dati sensibili (server e apparati di rete). Per l'installazione o modifica dei sistemi è necessario l'intervento dei tecnici scelti dal comune per l'assistenza.
5	1	2	M		Vedi 5.1.1 – Gli accessi vengono sempre registrati dai sistemi di log già presenti nei sistemi operativi o negli apparati di rete.
5	1	3	S		
5	1	4	A		
5	2	1	M		Al momento esiste solamente una utenza amministrativa per dispositivo o sistema.
5	2	2	A		
5	3	1	M		I nuovi dispositivi quando entrano a far parte del dominio del comune ricevono già le configurazioni di amministrazione del dominio.
5	4	1	S		
5	4	2	S		
5	4	3	S		
5	5	1	S		
5	6	1	A		
5	7	1	M		Le credenziali definite sono di elevata robustezza, ma non arrivano a 14 caratteri, sistemeremo il prima possibile.
5	7	2	S		
5	7	3	M		Al momento non è predisposto una scadenza delle password, sistemeremo il prima possibile.

5	7	4	M	Questo è un'impostazione predefinita dei sistemi operativi Windows, che sono i sistemi utilizzati dal comune.
5	7	5	S	
5	7	6	S	
5	8	1	S	
5	9	1	S	
5	10	1	M	Le utenze sono suddivise in gruppi e identificate.
5	10	2	M	Al momento non è così, sistemeremo il prima possibile.
5	10	3	M	Al momento non è così, sistemeremo il prima possibile.
5	10	4	S	
5	11	1	M	Il comune di Busseto è in regola.
5	11	2	M	Il comune di Busseto è in regola.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID	Livello	Descrizione	Modalità di implementazione	
8	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 ogni postazione e sul server è installato un software antivirus.
8	1	M	Installare su tutti i dispositivi firewall ed IPS personali.	Il comune ha un Firewall fisico e sulle postazioni c'è anche il firewall presente nel software antivirus.

8	1	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	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	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	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Il comune di Busseto è in regola.
8	3	A	Monitorare l'uso e i tentativi di utilizzo di	

			dispositivi esterni.	
8	4	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	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	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	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	

8	7	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Al momento non è predisposta una configurazione simile sui vari dispositivi. Sistemeremo il prima possibile.
8	7	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Le macro sono disattivate per impostazione predefinita dei software del pacchetto Microsoft Office.
8	7	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	La posta utilizzata dal comune è letta dal Browser, e per impostazione predefinita i messaggi non vengono aperti automaticamente.
8	7	M	Disattivare l'anteprima automatica dei contenuti dei file.	Al momento non è predisposta una configurazione simile sui vari dispositivi. Sistemeremo il prima possibile.
8	8	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Al momento non è predisposta una configurazione simile sui vari dispositivi. Sistemeremo il prima possibile.
8	9	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario,	La posta utilizzata dal comune è filtrata da un sistema antispam.

			prevedendo anche l'impiego di strumenti antispam.	
8	9	M	Filtrare il contenuto del traffico web.	Il traffico Web viene filtrato dal Firewall fisico presente in comune.
8	9	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).	L'antispam effettua già scansione e blocco di file potenzialmente pericolosi (.exe, .dat, .cab, etc…).
8	10	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	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	M	Effettuare almeno	Il comune dispone di un

			settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	sistema di Backup che fa una copia di sicurezza di tutto il server, garantendo la possibilità di recupero dei dati e ripristino del sistema in caso di rottura.
10	1	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	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	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	Il backup viene cifrato e può essere letto solamente utilizzando il sistema che lo ha fatto.

			trasmissione consente la remotizzazione del backup anche nel cloud.	
10	4	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.	La copia offsite deve essere predisposta. Per questo è necessario anche l'acquisto di Dischi USB. Sistemeremo il prima possibile.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID	Livello	Descrizione	Modalità di implementazione	
13	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	Poiché la quantità di dati è gestibile, si può optare per la crittografia di tutto il backup. Da definire con il responsabile del comune di Busseto.
13	2	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	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	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	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	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	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	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il Firewall utilizza un sistema di blacklist pubbliche e di categorie di siti per bloccare quelli potenzialmente pericolosi.
13	9	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.	