MISURE MINIME DI SICUREZZA ICT

Compilare ed inviare a rpd@euservice.it

Istituzione scolastica	I. C. "Piazza Borgoncini Duca"		**Codice Meccanografico**	rmic847005	
Referente informatico	STEFANIA FILIPPONI	6390421	rmic847005@istruzione.it	**Data di compilazione**	05/11/18
	Cognome e nome	*Telefono*	*email*		

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Esempio di modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L’inventario delle risorse di segreteria (1 server e 8 client) elenca i dispositivi informatici collegati in rete in modo permanente e/o provvisorio e riporta: • Tipo di apparato e codice identificativo assegnato • Descrizione breve del tipo di dispositivo • Collocazione dell’apparato • Persona alla quale è assegnato il client. L'inventario delle risorse assegnate alla didattica elenca i dispositivi presenti nelle aule attrezzate e nei laboratori.	L’inventario delle risorse di segreteria è essere riportato in una scheda ad hoc. L’inventario elenca i dispositivi informatici collegati in rete in modo permanente e/o provvisorio ed essere strutturato nel modo seguente: • Tipo di apparato e codice identificativo assegnato • Descrizione breve del tipo di dispositivo • indirizzo IP • Collocazione dell’apparato • Persona alla quale è assegnato in caso di client E' implementato con la stessa metodologia anche un elenco dei dispositivi collegati alla didattica
1	3	1	M	Aggiornare l’inventario quando nuovi dispositivi approvati vengono collegati in rete.	L’elenco delle risorse di cui alla misura 1.1.1 è aggiornato con l'aggiunta di nuove risorse. E' implementato con la stessa metodologia l’aggiornamento dell’elenco dei dispositivi collegati alla didattica	L’elenco delle risorse di cui alla misura 1.1.1 è aggiornato con l'aggiunta di nuove risorse. E' implementato con la stessa metodologia l’aggiornamento dell’elenco dei dispositivi collegati alla didattica
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.
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’istallazione di software non compreso nell’elenco.	L’inventario contiene: • Nome del software e dove è installato Sono fornite istruzioni al personale circa il divieto di installare software diversi da quelli inventariati. Le esigenze di nuovi software sono vagliate dall' amministratore di sistema, che eventualmente provvede all'installazione e ad aggiornare l'inventario. Le abilitazioni all’installazione del software sono concesse solamente agli amministratori di sistema Viene implementato con la stessa metodologia l’aggiornamento dell’elenco dei software collegati alla didattica	L’inventario contiene: • Nome del software • Fornitore e/o marca • Versione del software • Dove è installato il software • Dove sono archiviati i dati prodotti dal software • Sistemi di copia di dati prodotti dal software. Sono fornite istruzioni al personale circa il divieto di installare software diversi da quelli inventariati. Le esigenze di nuovi software sono vagliate agli amministratore di sistema, che eventualmente provvede all'installazione e ad aggiornare l'inventario. Le abilitazioni all’installazione del software sono concesse solamente agli amministratori di sistema (vedi 5.1.1). Viene implementato con la stessa metodologia l’aggiornamento dell’elenco dei software collegati alla didattica
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Nelle macchine di segreteria nessun utente ha l’abilitazione per installare nuovi software. Le scansioni vengono effettuate dai responsabili della sicurezza del sistema informatico. Per la didattica non sono attivi sistemi di scansione e la gestione può essere lasciata ai docenti ed ai responsabili di laboratorio.	Nelle macchine di segreteria nessun utente ha l’abilitazione per installare nuovi software. Le scansioni vengono effettuate dai responsabili della sicurezza del sistema informatico. Per la didattica non sono attivi sistemi di scansione e la gestione può essere lasciata ai docenti ed ai responsabili di laboratorio.

	3	**1**	**1**	**M**	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutti i sistemi operativi installati hanno configurazione standard.	Tutti i sistemi operativi installati hanno configurazione standard. Per la rete di segreteria è aggiunto n antivirus per la navigazione in rete Sono utilizzate copie immagine conservate come descritto al punto 3.3.1 e 3.3.2.
	3	**2**	**1**	**M**	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di si- stemi usati dall'organizzazione.	Tutti i sistemi operativi installati hanno configurazione standard.	Vedi 3.1.1.
	3	**2**	**2**	**M**	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzan- do la configurazione standard.	Sono previste le misure minime sicurezza sistemi di backup e ripristino dati sia per i server che per i client della segreteria.	Devono prevedersi per le misure minime sicurezza sistemi di backup e ripristino dati sia per i server che per i client della segreteria. Per la parte didattica la gestione può essere lasciata ai docenti ed ai responsabili di laboratorio.
	3	**2**	**3**	**S**	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestio- ne dei cambiamenti.		
	3	**3**	**1**	**M**	Le immagini d'installazione devono essere memorizzate offline.	Nel Disciplinare Tecnico sono descritte le modalità di conservazione dell immagini dei server e dei PC della segreteria. Tale procedura non è prevista per la rete della didattica.	Nel Disciplinare Tecnico sono descritte le modalità di conservazione dell immagini dei server e dei PC della segreteria. Tale procedura non è prevista per la rete della didattica.
	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).	Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…) Tutte le operazioni di amministrazione remota sono svolte solo attraverso connessioni protette e sicure. La rete didattica è separata da quella della segreteria.	Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…) Tutte le operazioni di amministrazione remota sono svolte solo attraverso connessioni protette e sicure. La rete didattica è separata da quella della segreteria.
	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.	Per la segreteria si utilizza un software antivirus in aggiunta ad un software di scansione di vulnerabilità. Per la didattica non sono necessari software specifici. I responsabili di laboratorio e gli operatori di segreteria devono essere informati sulla necessità di monitorare tutti i sistemi in rete, a fronte di una significativa modifica (installazione di un sistema o software nuovo, aggiornamento, modifica della configurazione) di uno o più sistemi o software.	Per la segreteria si utilizza un software antivirus in aggiunta ad un software di scansione di vulnerabilità. Per la didattica non sono necessari software specifici. I responsabili di laboratorio e gli operatori di segreteria devono essere informati sulla necessità di monitorare tutti i sistemi in rete, 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	**4**	**1**	**M**	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Sono date disposizioni agli operatori affinché verifichino che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.	Devono essere date disposizioni agli operatori affinché verifichino che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.
	4	**5**	**1**	**M**	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'applicazione delle patch di vulnerabilità per la segreteria deve essere in carico dell'amministratore di sistema, per la didattica degli animatori digitali e dei responsabili di laboratorio. In quest'ultimo caso qualora l'applicazione automatica delle patch non abbia successo o possa provocare gravi problemi al funzionamento dei sistemi, potrà essere necessario bloccare l'attività di patching e far intervenire personale adeguatamente preparato per la soluzione.	L'applicazione delle patch di vulnerabilità per la segreteria deve essere in carico dell'amministratore di sistema, per la didattica degli animatori digitali e dei responsabili di laboratorio. In quest'ultimo caso qualora l'applicazione automatica delle patch non abbia successo o possa provocare gravi problemi al funzionamento dei sistemi, potrà essere necessario bloccare l'attività di patching e far intervenire personale adeguatamente preparato per la soluzione.
	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.		I dispositivi air-gapped sono a reti wi-fi separate dalla rete della segreteria.

	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.	Sono presenti disposizioni ai responsabili di laboratori e agli operatori di segreteria affinché contattino l'amministratore di sistema per la risoluzione delle vulnerabilità non corrette da patch o altri sistemi. L'amministratore di sistema provvede alla definizione delle ulteriori misure aggiuntive.	Sono presenti disposizioni ai responsabili di laboratori e agli operatori di segreteria affinché contattino l'amministratore di sistema per la risoluzione delle vulnerabilità non corrette da patch o altri sistemi. L'amministratore di sistema provvede alla definizione delle ulteriori misure aggiuntive.
	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.).	E' redatto un documento per la gestione del rischio informatico.	E' redatto un documento per la gestione del rischio informatico.
	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.	E' redatto un documento per la gestione del rischio informatico.	Vedi 4.8.1
	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.	I privilegi di amministrazione sono limitati agli addetti di segreteria e ai responsabili dei laboratori informatici.	I privilegi di amministrazione sono limitati agli addetti di segreteria e ai responsabili dei laboratori informatici.
	5	**1**	**2**	**M**	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Gli accessi sono controllati da un server di dominio.	Gli accessi sono controllati da un server di dominio.
	5	**2**	**1**	**M**	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I documenti di nomina dei responsabili di laboratorio e degli assistenti amministrativi sono consegnati agli stessi e una copia è conservata in segreteria.	I documenti di nomina dei responsabili di laboratorio e degli assistenti amministrativi sono consegnati agli stessi e una copia è conservata in segreteria.
	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 operatori sono impartite adeguate istruzioni al riguardo.	Agli operatori sono impartite adeguate istruzioni al riguardo.
	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).	Sono fornite indicazioni a tutti gli utenti per l'utilizzo di password di autenticazioni "forti", "almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola"	Devono essere fornite indicazioni a tutti gli utenti per l'utilizzo di password di autenticazioni "forti", "almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola"
	5	**7**	**3**	**M**	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
	5	**7**	**4**	**M**	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Sono fornite indicazioni a tutti gli utenti per impedire il riutilizzo delle ultime 6 password.	Sono fornite indicazioni a tutti gli utenti per impedire il riutilizzo delle ultime 6 password.
	5	**10**	**1**	**M**	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Agli operatori di segreteria e ai responsabili di laboratorio sono impartite adeguate istruzioni al riguardo.	Agli operatori di segreteria e ai responsabili di laboratorio sono impartite adeguate istruzioni al riguardo.
	5	**10**	**2**	**M**	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze di segreteria sono assegnate alla singola persona. Tale livello di protezione non è necessario nella rete didattica.	Le utenze di segreteria sono assegnate alla singola persona. Tale livello di protezione non è necessario nella rete didattica.

	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.	Le utenze amministrative anonime sono utilizzate solo per situazioni di emergenza dagli amministratori di sistema.	Le utenze amministrative anonime sono utilizzate solo per situazioni di emergenza dagli amministratori di sistema.
	5	**11**	**1**	**M**	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Sono raccolte in busta chiusa e conservate dal responsabile del trattamento in un luogo sicuro.	Sono raccolte in busta chiusa e conservate dal responsabile del trattamento in un luogo sicuro.
	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 di amministrazione se non quelle di sistema.	Non si utilizzano certificati digitali per l’autenticazione delle utenze di amministrazione se non quelle di sistema.
	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, portatili e server della segreteria sono installati antivirus con aggiornamento automatico.	Su tutti i PC, portatili e server della segreteria sono installati antivirus con aggiornamento automatico.
	8	**1**	**2**	**M**	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC, portatili e server sono attivati firewall locali.	Su tutti i PC, portatili e server sono attivati firewall locali.
	8	**3**	**1**	**M**	Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali.	Sono fornite disposizioni al personale di segreteria circa la limitazione all'uso di dispositivi esterni non necessari per le attività di segreteria. Tale disposizione non è prevista per la rete didattica.	Sono fornite disposizioni al personale di segreteria circa la limitazione all'uso di dispositivi esterni non necessari per le attività di segreteria. Tale disposizione non è prevista per la rete didattica.
	8	**7**	**1**	**M**	Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Sono fornite disposizioni al personale di segreteria.	Sono fornite disposizioni al personale di segreteria.
	8	**7**	**2**	**M**	Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.
	8	**7**	**3**	**M**	Disattivare l’apertura automatica dei messaggi di posta elettronica.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.
	8	**7**	**4**	**M**	Disattivare l’anteprima automatica dei contenuti dei file.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.
	8	**8**	**1**	**M**	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.	Sono fornite disposizioni al personale di segreteria. Le eventuali eccezioni sono valutate dall'amministratore di sistema.
	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.	La scuola utilizza il servizio di posta elettronica ministeriale e certificata(PEC) che include il filtraggio richiesto.	La scuola utilizza il servizio di posta elettronica ministeriale e certificata(PEC) che include il filtraggio richiesto.

8	**9**	**2**	**M**	Filtrare il contenuto del traffico web.	L’antivirus include funzioni di filtro alla navigazione. Inoltree sono fornite istruzioni agli operatori per configurare il software antivirus delle postazioni di lavoro.	L’antivirus include funzioni di filtro alla navigazione. Inoltree sono fornite istruzioni agli operatori per configurare il software antivirus delle postazioni di lavoro.
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).	L’antivirus include funzioni di filtro alla navigazione. Inoltree sono fornite istruzioni agli operatori per configurare il software antivirus delle postazioni di lavoro	L’antivirus include funzioni di filtro alla navigazione. Inoltree sono fornite istruzioni agli operatori per configurare il software antivirus delle postazioni di lavoro.
10	**1**	**1**	**M**	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	I sistemi di copia di sicurezza sono descritti in un Disciplinare Tecnico e le attività di copia registrate in un registro. Nello stesso documento sono descritti anche il disaster recovery ed i tempi di ripristino del sistema.	I sistemi di copia di sicurezza sono descritti in un Disciplinare Tecnico e le attività di copia registrate in un registro. Nello stesso documento sono descritti anche il disaster recovery ed i tempi di ripristino del sistema.
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.	Nel Disciplinare Tecnico sono descritte le modalità per il rispetto del requisito di protezione delle copie di sicurezza.	Nel Disciplinare Tecnico sono descritte le modalità per il rispetto del requisito di protezione delle copie di sicurezza.
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.	Nel Disciplinare Tecnico sono descritte le modalità per il rispetto del requisito di protezione delle copie di sicurezza.	Nel Disciplinare Tecnico sono descritte le modalità per il rispetto del requisito di protezione delle copie di sicurezza.
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	Nella rete di segreteria l’analisi dei livelli particolari di riservatezza è garantita con la compartimentazione dei dati in cartelle il cui accesso è fisicamente controllato e protetto da password e dal profilo utente. Per la didattica non si prevedono sistemi di scansione attivi e la gestione viene attualmente lasciata ai docenti ed ai responsabili di laboratorio.	Nella rete di segreteria l’analisi dei livelli particolari di riservatezza è garantita con la compartimentazione dei dati in cartelle il cui accesso è fisicamente controllato e protetto da password e dal profilo utente. Per la didattica non si prevedono sistemi di scansione attivi e la gestione viene attualmente lasciata ai docenti ed ai responsabili di laboratorio.
13	**8**	**1**	**M**	Bloccare il traffico da e verso url presenti in una blacklist.	Il blocco del traffico da e verso url presenti nella blacklist è implementata sul Firewall.	Il blocco del traffico da e verso url presenti nella blacklist è implementata sul Firewall.