ISTITUTO ISTRUZIONE SUPERIORE
GUIDO MONACO DI POMPOSA
V.le della Resistenza, 3
40021 CODIGORO (FE)

MISURE MINIME PER LA SICUREZZA ICT
nelle pubbliche amministrazioni

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 attive redatto con il software freeware "Advanced IP Scanner".
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Lo strumento automatico adottato è il software "Advanced IP Scanner" di Famatech Corp.
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 logging è registrato dal firewall di rete.
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.	In caso di collegamento in rete di nuovi dispositivi approvati viene lanciata una nuova scansione con il sw "Advanced IP Scanner"
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Strumento adottato è il sw "Advanced IP Scanner"
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.	Il software utilizzato per la scansione produce report che possono essere stampati.

1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	//
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	//
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Al momento l'autenticazione a livello di rete esiste per il solo sistema wi-fi.
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.	Si allega al presente documento l'elenco dei software (allegato nr. 1) utilizzati per esigenze amministrative.

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.	Vengono effettuate scansioni con il software freeware “WinAudit” installato in locale su ogni pc.
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.	Si procede rimuovendo il software non necessario dal sistema; vengono disattivati servizi servizi, moduli del kernel, e i protocolli non necessari; configurazione del personal firewall
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.	Vengono configurati utenti standard con rimozione degli utenti non necessari; abilitazione dei log di sicurezza; installazione delle patch di sicurezza.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono	Per il server della Segreteria le configurazioni standard vengono salvate su immagini generate con l'utility "Windows Server

				essere ripristinati utilizzando la configurazione standard.	Backup"; per i client con l'utility "Ripristino configurazione di sistema"; i client amministrati dal dominio Microsoft hanno apposite policy che definiscono la configurazione standard rendendo inutile la creazione di apposite immagini.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	//
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione non accessibili direttamente.
//	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 remota viene effettuata con il software commerciale "Supremo" della Nanosystem.
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.	Ricerca delle vulnerabilità effettuata con gli strumenti software freeware “Nmap Security Scanner” e “Nessus Home”
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Viene effettuata una ricerca mensile delle vulnerabilità di rete con gli strumenti software freeware “Nmap Security Scanner”e “Nessus Home”
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.	Aggiornamento mensile degli strumenti software “Nmap Security Scanner”e “Nessus Home” utilizzati per la ricerca delle vulnerabilità.
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.	Gli aggiornamenti automatici dei sistemi operativi e degli applicativi sono sempre attivi in Segreteria
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.	Aggiornamenti manuali effettuati regolarmente su tali sistemi attraverso patch trasferite con USB Key o condivisioni di rete
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	//
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Vulnerabilità risolte per mezzo delle apposite patch di sistema o riconfigurazione del dispositivo di rete vulnerabile o aggiornamento firmware
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.).	Vedi piano di gestione dei rischi. Allegato nr 2
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 piano di gestione dei rischi. Allegato nr 2

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

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Gli operatori utilizzano account limitati per le consuete attività didattiche e amministrative: soltanto l'amministratore di sistema utilizza account amministrativi. Il gestionale cloud per la Segreteria Digitale di ARGO consente di profilare ciascun utente in modo granulare, tramite un sistema puntuale di permessi e profili, al fine di gestire i privilegi per ogni funzionalità del software.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Utenze amministrative utilizzate dall'amministratore di sistema per le sole operazioni di configurazione, accessi registrati nel log degli eventi di sistema di server e client. Nuvola registra gli accessi effettuati in modo automatico.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Per quanto riguarda il gestionale ARGO, vedi punto 5.1.1M

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.	Vedi elenco allegato di tutte le utenze amministrative degli uffici di segreteria. E' possibile controllare tutte le utenze all'interno delle funzioni di ARGO di gestione degli utenti e dei ruoli, verificando anche la data dell'ultimo accesso.
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.	Operazione effettuata sistematicamente per ogni dispositivo nuovo connesso alla rete
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.	Traccia presente nei log degli eventi di sistema di server e client
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).	Adeguata la complessità delle password delle utenze amministrative di Segreteria. ARGO obbliga ad impostare una password alfanumerica di almeno 7 caratteri
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	I requisiti di complessità delle password delle utenze amministrative vengono già controllate dall'amministratore di rete
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Attivazione policy sul server di dominio per il cambio automatico delle password delle utenze amministrative ogni 3 mesi. In ARGO verrà implementata a breve tale funzionalità
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Attivazione policy sul server di dominio per il cambio automatico delle password delle utenze amministrative con password history. In Nuvola verrà implementata a breve tale funzionalità.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Attivazione policy sul server di dominio per la durata minima delle password delle utenze amministrative
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.	Esecuzione di tutte le attività amministrative dall'utente standard con l'opzione "Esegui come Amministratore"
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.	Elenco completo delle utenze amministrative dell'Ufficio Segreteria, allegato al presente documento. In ARGO ad ogni utenza corrispondono privilegi diversi e quindi ogni utenza è distinta dalle altre ed ha diverse credenziali.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Utenze amministrative riconducibili alla persona cui sono assegnate con apposita denominazione specifica (nome). In ARGO ogni utenza è legata ad una singola anagrafica del personale.
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.	Utenze amministrative anonime utilizzate per emergenza dal solo Amministratore di sistema
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).	Nel dominio della Segreteria si utilizzano le utenze amministrative del dominio stesso
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono depositate in cassaforte. In ARGO le credenziali sono conservate in forma criptata all'interno della base dati di ARGO stesso e quindi sono accessibili solo tramite le funzioni del gestionale.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Certificati digitali presenti per Entratel, conservate in copia in cassaforte

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.	Antivirus Eset NOD32 installato su server e postazioni della Segreteria.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Personal firewall attivato su tutti i dispositivi di rete; Firewall di rete configurato a monte
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	//
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	//
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	//
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	//
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Si evita l'utilizzo di pen drive di provenienza esterna
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.	E' presente un firewall di rete.
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.	Il firewall di rete dispone di un servizio di "content filtering".
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	AutoPlay disattivato su tutte le postazioni (nel dominio della Segreteria con apposita policy sul server)
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Software con funzioni "macro" disattivate
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Anteprima dei client di posta elettronica utilizzati disattivata
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Anteprima dei contenuti dei file di immagine e pdf disattivata dal browser delle risorse di sistema
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	La scansione automatica dei supporti rimovibili viene effettuata automaticamente dal software antivirus impostato a tale scopo

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.	Filtro POP3 e antispam configurato nel client antivirus
8	9	2	M	Filtrare il contenuto del traffico web.	Antivirus dotato di protezione in tempo reale con filtro web attivo
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).	Tipi di file “a rischio” intercettati automaticamente dal client antivirus
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Scansione euristica attiva nella protezione in tempo reale del client antivirus
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.	Copie di sicurezza effettuate quotidianamente di tutto il contenuto del server della Segreteria. In ARGO vengono mantenuti tutti i backup di qualsiasi momento temporale degli ultimi 5 giorni. Viene inoltre effettuato un backup giornaliero, mantenuto per 1 anno.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema	Backup completo del server della Segreteria quotidiano. In ARGO vengono fatti test periodici di ripristino di tutti i dati di un

				operativo, le applicazioni software e la parte dati.	precedente backup al fine di verificare la possibilità di ripristinare l'intero sistema in caso di disaster recovery.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Backup del server della Segreteria effettuato sia con lo strumento "Windows Server backup" sia con lo strumento "Veeam backup", per il disaster recovery. In ARGO i backup vengono effettuati con strumenti diversi e l'integrità dei dati nel backup viene verificato con appositi software automatici.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Test di ripristino effettuati mensilmente. Per quanto riguarda ARGO, vedi 10.1.2°.
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.	Contenuti dei dispositivi di backup opportunamente cifrati. In ARGO i backup sono accessibili solo al fornitore del software. La comunicazione tra la produzione del backup e lo storage avviene tramite HTTPS.
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.	Supporti di backup non direttamente accessibili dal sistema. In ARGO i backup vengono gestiti in storage diversi da quelli dell'infrastruttura di ARGO.

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	Protezione applicata indistintamente su tutti i files

				segnatamente quelli ai quali va applicata la protezione crittografica	
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.	Filtro dei contenuti attivo sul firewall di rete
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.	//

Allegato nr. 1

ELENCO SOFTWARE UTILIZZATI NELLE SEGRETERIE

Sistemi operativi

Windows Server 2012 R2
Windows 10
Windows 7

Segreteria Digitale - Applicazione ARGO
Microsoft Office 2003
Microsoft Office 2007
Libre Office
Entratel – Desktop Telematico (applicazione Agenzia delle Entrate)
UniEmens (applicazione INPS)
Adobe Acrobat Reader
Supremo (assistenza remota)
Avanced IP Scanner
WinAudit
Nessus

Eset NOD32 – Antivirus

ELENCO UTENZE AMMINISTRATIVE

UTENTI CON PRIVILEGI DI AMMINISTRAZIONE

ADMINISTRATOR (AMMINISTRATORE DI RETE)

marco.verri

Tutti gli altri utenti, sempre caratterizzati dall'account *nome.cognome o nome*, hanno permessi limitati e corrispondono agli impiegati delle segreterie e alla DSGA.
Questi utenti vengono disabilitati/cancellati nel momento in cui termina il contratto di lavoro.

Allegato nr. 2

PIANO DI CONTINUITÀ OPERATIVA E GESTIONE DEI RISCHI

L'obiettivo del piano di continuità operativa è quello di garantire la continuità del servizio informatico e la disponibilità delle informazioni, evitando o limitando i danni al patrimonio informativo a fronte di una emergenza.
Il ripristino è un processo di ricostruzione dell'operatività dell'infrastruttura a seguito dell'evento dannoso.
Si ha bisogno di un piano di continuità operativa e ripristino in caso di danneggiamento delle risorse (dati o strumenti), come ad esempio:

- Failure delle apparecchiature (es. disk crash)
- Rottuta dei power supply o apparecchiature di telecomunicazione
- Failure degli applicativi o corruzione dei database
- Errori umani, sabotaggio
- Malicious Software (Viruses, Worms, Trojan horses)
- Hacking o altri attacchi Internet attacks
- Social engineering
- Eventi naturali: acqua, fuoco, terremoti, intemperie

Il piano di continuità operativa e ripristino non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime.

Le misure di sicurezza preventive, che rilevano e/o riducono l'impatto, adottate dall'Istituto di Istruzione Superiore Guido Monaco di Pomposa sono:

- Auditing: tutte le misure di sicurezza adottate vengono verificate periodicamente;
- Aggiornamenti software di base e applicativo;
- Aggiornamenti antivirus;
- Manutenzione periodica di reti e sistemi;
- Gruppo di continuità;
- Salvataggio regolare dei dati.

Qualora emergesse un possibile problema di sicurezza, è prevista l'attivazione di un TEAM di Risposta per la gestione degli incidenti, guidato dall'incaricato del sistema informativo e della sicurezza dei dati.

CRITERI E MODALITÀ PER IL SALVATAGGIO E IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

DOMINIO GMU

E' stato creato il dominio GMU per adempiere alle regole dettate dal D.Lgs 196/03.

Sul server degli uffici è stato installato ACTIVE DIRECTORY per la gestione degli utenti.

Viene sincronizza l'orario dei client con il server.

Sono stati installati:

- Antivirus Eset NOD32
- Advanced IP Scanner per l'inventario delle risorse attive.
- WinAudit per l'esecuzione delle scansioni finalizzate alla rilevazione della presenza di software non autorizzato.

Gli utenti effettuano il log in con:
Nome.Cognome o nome pw: xxxxxx che poi verrà automaticamente ogni 3 mesi.
Sono statl adeguati i requisiti (obbligatori) che deve avere la PW: alfanumerica, con almeno 1 carattere maiuscolo, minimo 8 caratteri. Il sistema ricorda le ultime 5 pw, per cui, cambiandole, non è possibile utilizzarne una identica alla precedente. La validità minima delle pw è di 10gg, quella max è di 60 gg (per trattamento dati sensibili)

Ogni utente fa parte dei gruppi di protezione globale: Domain Users e Uffici.
Gli utenti creati possono accedere a tutti i computer del dominio; è possibile, però, limitare l'accesso solo al PC da loro usato e definire anche gli eventuali orari di lavoro. (tutto questo viene fatto da active directory).

LA RETE E I SISTEMI

Il Sistema Informativo dell'ISTITUTO DI ISTRUZIONE Superiore Guido Monaco di Pomposa è costituito da 2 reti locali:

- Rete amministrativa
- Rete wifi per la gestione del registro elettronico

RETE AMMINISTRATIVA

Viene utilizzata da:

- ✓ personale di segreteria didattica,
- ✓ personale di segreteria amministrativa
- ✓ DSGA
- ✓ Vicepresidenza

- ✓ Dirigente Scolastico

E' costituita da un server PDC (Windows 2012 R2 server Standard) che gestisce gli account (amministrativi e di dominio), e 8 client con sistemi operativi Windows 7 e Windows 10.
Chiunque è abilitato tramite ACTIVE DIRECTORY ad accedere a qualsiasi postazione di lavoro, ma sul desktop avrà un numero limitato di applicazioni in funzione al profilo utente.
La connettività Internet avviene attraverso il firewall su rete Lepida. Tutti i dati personali sono memorizzati sui server e quotidianamente si provvede a copia di backup.

RETE WIFI

E' utilizzata dai docenti con i notebook acquistati per il registro elettronico.

MANUTENZIONE PARCO MACCHINE

La manutenzione di primo livello dei server viene effettuata dal produttore/fornitore.
Per quanto riguarda i client, l'assistenza di primo livello e la manutenzione viene effettuata da un'Azienda esterna.

GLI APPLICATIVI

AUTENTICAZIONE AL DOMINIO

Esiste una procedura formalizzata di consegna dei PC che prevede l'assegnazione di uno User ID e di una password provvisoria che deve essere subito modificata dall'utente.
Chiunque, purché abilitato a mezzo Active Directory, ha accesso a un insieme ben identificato di funzioni (tipicamente Internet, Posta elettronica), anche sugli altri client collegati alla rete amministrativa.
Tutte le password di autenticazione al dominio sono alfanumeriche e almeno di 8 caratteri.
Esiste un meccanismo di scadenza automatica delle password di autenticazione al dominio (60giorni).

AUTORIZZAZIONE PER L'ACCESSO A BANCHE DATI/APPLICAZIONI

Tutte le procedure applicative gestite dal Personale tecnico prevedono User ID e Password, diverse da quelle di autenticazione.
La scadenza automatica delle password di autorizzazione è di 90 giorni.
Esiste una procedura formalizzata che consente all'Amministratore di sistema di resettare le password previa autorizzazione del Responsabile.

ANTIVIRUS

La protezione di tutti i posti di lavoro collegati alla rete amministrativa viene assicurata attraverso l'antivirus Eset NOD32 che garantisce l'aggiornamento automatico del database dei virus attivato con frequenza giornaliera.
La scansione sui posti di lavoro viene effettuata con frequenza giornaliera.
La protezione di tutti i posti di lavoro collegati alla rete didattica viene assicurata attraverso antivirus locali aggiornati periodicamente.

AGGIORNAMENTI SOFTWARE

Server

Software di base

Quando viene rilasciata una patch, questa viene verificata a cura dei manutentori esterni.

Software applicativo

Gli aggiornamenti delle patch sono a cura dei manutentori esterni.

Client

Gli aggiornamenti sul sistema operativo vengono effettuati in maniera automatica con l'impostazione delle operazioni pianificate del sistema operativo a cura dei Manutentori esterni.

Prot. n° 10579/I del 29.12.2017