Misure Minime di sicurezza ICT per le PA

SCUOLE ANNESSE ALL'EDUCANDATO SS. ANNUNZIATA

Acronimi utilizzati nelle Circolari ufficiali e nel resto del presente documento

Sigla	Significato	Note
ABSC	AgID Basic Security Control(s)	Controlli di sicurezza previsti dall'AgID
CSC	Critical Security Control(s)	Controlli di sicurezza critici, ritenuti fondamentali
CSSC	CIS - Critical Security Controls for Effective Cyber Defense	Controlli di sicurezza critici per una protezione funzionale dagli attacchi cibernetici

Livelli di sicurezza utilizzati nel presente documento

Nel documento, per ogni singola implementazione tecnica, è indicato il livello di sicurezza relativo. Le misure previste dal livello minimo devono essere messe in atto quanto prima, poiché ritenute necessarie dall'AgID.

Sigla	Note
M	Livello sotto il quale nessuna amministrazione può scendere: i controlli indicati debbono riguardarsi come **obbligatori**
S	Base di riferimento per un livello di sicurezza completo. Rappresenta il primo step a cui tendere per la protezione della propria infrastruttura informatica
A	Obiettivo finale a cui tendere, al completamento del piano di sicurezza

Nel corso del documento sono state evidenziate con diversi colori le singole misure previste, in modo da fornire un veloce colpo d'occhio su quanto sia:

- strettamente necessario: rosso
- da programmare: azzurro
- obiettivo finale: verde

Tempi di implementazione

La tabella proposta dall'AgID è stata integrata con una colonna che permette all'Amministrazione di specificare i tempi di messa in opera di ogni misura di sicurezza.

Sigla	Descrizione
II	Implementazione **Immediata**. Da mettere in atto quanto prima per raggiungere il livello minimo richiesto
ID	Implementazione in itinere, **durante** la validità del piano di sicurezza informatica
IS	Implementazione a **scadenza**, da realizzarsi entro il termine di validità del piano di sicurezza informatica

Note specifiche programmi Argo e Nettuno e Suite Nettuno

I programmi Argo e Nettuno in Cloud, così come i futuri sviluppi della tecnologia Argo e Nettuno in cloud sono installati e gestiti all'interno del data center di uno dei più grandi fornitori di servizi WEB collocato sul territorio nazionale: Infocert si è dotata della certificazione ISO 27001:2013 e degli altri mezzi e/o strumenti ritenuti idonei a tutelare nella maniera più efficace la sicurezza delle informazioni (fisica, logica, informatica ed organizzativa). Il servizio utilizzato da Argo e Nettuno è *Server Dedicati, Housing e Colocation*.

La Piattaforma Cloud attraverso la quale è erogato il servizio Suite Nettuno è Aruba s.p.a. A garanzia di sicurezza ed affidabilità il Registro Elettronico NETTuno è stato il primo ad ottenere la qualificazione Agid il 12-03-2019.

Tutti i dati archiviati e i backup sono protetti con la crittografia, mediante l'Advanced Encryption Standard AES-256. Il sistema di gestione adottato consente di avere una facile ridondanza e replicazione dei sistemi informatici e dei dati, preservando così i clienti da rischi di interruzione prolungata dei servizi e/o di perdita delle informazioni.

ABSC_ID	Livello	Descrizione	Modalità implementazione	Tempi

		n e		
1	1	M	L'amministratore di rete fornisce elenco dei server, dei PC e dei dispositivi (stampanti, scanner, NAS, Access Point, switch) presenti nella rete	II
1	1	S	L'amministratore di rete installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	1	A	L'amministratore di rete installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	1	A	L'amministratore di rete installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	2	S	L'amministratore di rete attiva i LOG del server DHCP, se presente	IS
1	2	S	L'amministratore di rete verifica periodicamente i log e li confronta con i propri elenchi di dispositivi	ID
1	3	M	L'amministratore di rete aggiorna la documentazione	II
1	3	S	L'amministratore di rete aggiorna la documentazione	IS
1	4	M	L'amministratore di rete aggiorna la documentazione	II

1	4	S	L'amministratore di rete aggiorna la documentazione	IS
1	4	A	L'amministratore di rete aggiorna la documentazione e verifica periodicamente i log dei dispositivi che hanno utilizzato la rete	IS
1	5	A	L'amministratore di rete verifica che nelle reti WIFI sia presente un sistema di autenticazione Captive Portal basato su account singoli e non su chiave WPA/WPA2 comune	IS
1	6	A	L'amministratore verifica l'esistenza (ove possibile) di certificati lato client.	IS

ABSC_ID	Livello	Descrizione	Modalità implementazione	Tempi
2	1	M	L’amministratore di rete aggiorna la documentazione	II
2	2	S	L’amministratore di rete aggiorna la documentazione	IS
2	2	S	L’amministratore di rete aggiorna la documentazione	IS
2	2	A	L’amministratore di rete utilizza strumenti hardware/software di checksum sui repository software	IS
2	3	M	L’amministratore di rete verifica le applicazioni installate	II

2	3	S	L’amministratore di rete aggiorna la documentazione	IS
2	3	A	L’amministratore di rete predispone su un server apposito degli strumenti per l’analisi delle configurazioni software della rete	IS

2	4	A	L’amministratore di rete verifica se esistono applicazioni di questo tipo e predispone i dovuti accorgimenti di protezione	IS

ABSC_ID			Livello	Descrizione	Tempi	
3	1	1	M		L’amministratore di rete impartisce istruzioni su come gestire i singoli sistemi operativi	II
3	1	2	S		L’amministratore di rete, all’atto dell’installazione di una nuova postazione, verifica che siano rispettate le procedure di hardening: eliminazione account non necessari disabilitazione servizi non necessari chiusura porte di rete non necessarie	ID
3	1	3	A		L'amministratore di rete redige un documento in cui si definisce la configurazione standard delle workstation della rete e predispone una configurazione standard	IS
3	2	1	M		L’amministratore di rete redige un documento in cui si definisce la configurazione standard delle workstation della rete	II
3	2	2	M		L’amministratore di rete definisce le procedure di ripristino	II
3	2	3	S		L’amministratore di rete definisce le procedure di ripristino	IS
3	3	1	M		L’amministratore di rete mantiene un archivio aggiornato delle immagini dei sistemi installati	II

3	3	2	S	L’amministratore di rete mantiene un archivio aggiornato delle immagini dei sistemi installati	IS

3	4	1	M	L'amministratore di rete verifica che su server e workstation siano utilizzati solo strumenti di amministrazione remota che rispettino i protocolli di connessione protetta	II
3	5	1	S	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	5	2	A	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	5	3	A	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	5	4	A	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	6	1	A	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	7	1	A	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS

ABSC_ID	Livello	Descrizione	Modalità di implementazione	Tempi
4	1	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'amministratore di rete verifica che siano impostate operazioni pianificate di verifica delle vulnerabilità (Antivirus, antimalware, etc)	II
4	1	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	L'amministratore di rete verifica che siano impostate operazioni pianificate di verifica delle vulnerabilità (Antivirus, antimalware, etc)	ID
4	1	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).	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	IS
4	2	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
4	2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
4	2	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID

4	3	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.	L’amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
4	3	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.	L’amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID

4	4	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici degli strumenti di scansione	II
4	4	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	L'amministratore di rete certifica di essere abbonato a un servizio online di informazioni sulla cybersicurezza	ID
4	5	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi	II
4	5	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi e provvede ad aggiornare i sistemi non collegati direttamente alla rete	II
4	6	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	L'amministratore di rete verifica i i log delle attività	ID
4	7	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.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi	II
4	7	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.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi e decide i livelli di rischio in base ai risultati emersi	ID

4	8	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.).	L'amministratore di rete stila un elenco delle modalità di gestione dei rischi	II
4	8	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.	L'amministratore di rete stila un elenco delle modalità di gestione dei rischi	II

4	9	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.	L’amministratore di rete stila un elenco delle modalità di gestione dei rischi	ID
4	10	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.	L’amministratore di rete certifica di essere in possesso di ambienti di test su cui valuta l’impatto di prodotti non standard sugli apparati della rete	IS

ABSC_ID			Livello	Descrizione	Tempi	
5	1	1	M		L'amministratore di rete verifica i privilegi degli account utente. I prodotti Argo e Nettuno e Nettuno consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD).	II
5	1	2	M		L'amministratore di rete verifica i privilegi degli account utente. I prodotti Argo e Nettuno e Nettuno registrano in automatico ogni accesso effettuato al sistema. Il sistema Argo e Nettuno Cloud e Nettuno Cloud possiede un log puntuale di tutte le operazioni effettuate e consente l'accesso allo stesso a qualsiasi richiesta proveniente dall'utente o dalle autorità preposte	II
5	1	3	S		L'amministratore di rete verifica i privilegi degli account utente. Vedi punto 5.1.1M	ID
5	1	4	A		L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi. I prodotti Argo e Nettuno e Nettuno registrano su tabella di log ogni singola operazione effettuata sui dati. La conservazione di tale log dipende dallo spazio presente sul disco del server della scuola e dalle impostazioni fornite dalla scuola stessa sulla grandezza massima del file di LOG. Il LOG gestito da Argo e Nettuno Cloud viene storicizzato ogni 3 mesi e collocato in stato di READONLY. Dopo 12 mesi viene cancellato	ID
5	2	1	M		L'amministratore di rete redige la documentazione della rete. Tramite la gestione utenti di Argo e Nettuno è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. Argo e Nettuno Cloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utente.	II

5	2	2	A	L'amministratore di rete redige la documentazione della rete e la mantiene aggiornata tramite strumenti software	IS
5	3	1	M	L'amministratore di rete verifica i privilegi degli account utente	II
5	4	1	S	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi. Vedi punto 5.1.4.A L'aggiunta o la soppressione di un'utenza amministrativa sono operazioni che vengono svolte sul DB e quindi regolarmente registrate nel file di LOG. Anche in Argo e Nettuno Cloud l'operazione viene regolarmente tracciata all'interno del file LOG.	ID
5	4	2	S	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi	IS
5	4	3	S	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi	IS
5	5	1	S	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi	IS
5	6	1	A	L'amministratore di rete verifica le modalità degli accessi amministrativi	IS

5	7	1	M	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Argo e Nettuno consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite: 1. Verifica o meno del doppio accesso 2. Inserimento data generale di scadenza password 3. Numero di gg massimi per la validità del codice di accesso 4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso 5. Lunghezza minima del codice di accesso (in questo caso 14) 6. Numero minimo dei caratteri minuscoli 7. Numero minimo dei caratteri maiuscoli 8. Numero minimo dei caratteri numerici 9. Numero minimo dei caratteri speciali	II
5	7	2	S	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. I parametri definiti in Argo e Nettuno al punto precedente (5.7.1.M) consentono di effettuare questo controllo in automatico impedendo di fatto l'utilizzo di credenziali deboli.	ID
5	7	3	M	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Vedi parametri indicati nel punto 5.7.1.M	II
5	7	4	M	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Argo e Nettuno gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza.	II

5	7	5	S	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003	ID
5	7	6	S	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003	ID
5	8	1	S	L'amministratore di rete verifica le modalità degli accessi amministrativi. Argo e Nettuno consentono, per le funzioni particolarmente delicate, di inserire un ulteriore codice di accesso. L'utente quindi dopo aver effettuato il login dovrà inserire anche un ulteriore codice di accesso per poter effettuare la funzione scelta.	IS
5	9	1	S	L'amministratore di rete verifica le modalità degli accessi amministrativi	IS
5	10	1	M	L'amministratore di rete verifica le modalità degli accessi amministrativi. La gestione degli amministratori rispetto alle normali utenze viene fatta, in Argo e Nettuno, tramite la gestione dei livelli (1-9 9=amministratore) e le tipologie di accesso per ogni utente/funzione (5.1.1M)	II
5	10	2	M	L'amministratore di rete verifica le modalità degli accessi amministrativi. In Argo e Nettuno, ad ogni utenza, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi Anche in Argo e Nettuno Cloud le utenze di accesso sono legate a precise anagrafiche presenti nel sistema	II

5	10	3	M	L’amministratore di rete verifica le modalità degli accessi amministrativi	II

5	10	4	S	L'amministratore di rete verifica le modalità degli accessi amministrativi	ID
5	11	1	M	L'amministratore di rete verifica le modalità degli accessi amministrativi. Per quanto concerne i prodotti Argo e Nettuno tali credenziali sono gestite all'interno della base dati, l'accesso alla stessa è consentito solo tramite i programmi Argo e Nettuno e quindi secondo le regole di sicurezza enunciate in questo documento. Anche per Argo e Nettuno Cloud vale lo stesso principio con l'aggiunta che la base dati non è in alcun modo accessibile a nessuno se non tramite programmi Argo e Nettuno e quindi secondo le regole indicate nel presente documento.	II
5	11	2	M	L'amministratore di rete verifica le modalità degli accessi amministrativi	II

ABSC_ID	Livello	Descrizione	Modalità di implementazione	Tempi
8	1	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.	L'amministratore di rete verifica la presenza di sistemi antivirus e firewall software locali	II
8	1	Installare su tutti i dispositivi firewall ed IPS personali.	L'amministratore di rete verifica la presenza di sistemi antivirus e firewall software locali	II
8	1	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	L'amministratore di rete installa e configura un sistema di gestione centralizzata dei log	IS
8	2	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	L'amministratore di rete verifica che gli antivirus locali siano gestibili attraverso un sistema centralizzato	ID
8	2	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.	L'amministratore di rete verifica che gli antivirus locali siano gestibili attraverso un sistema centralizzato	ID
8	2	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	L'amministratore di rete verifica che gli antivirus locali siano gestibili attraverso un sistema centralizzato	ID
8	3	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'amministratore di rete verifica l'utilizzo di dispositivi esterni	II
8	3	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	L'amministratore di rete verifica l'utilizzo di dispositivi esterni	IS

8	4	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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
8	4	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	ID

8	5	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
8	5	Installare sistemi di analisi avanzata del software sospetto.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
8	6	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
8	7	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	7	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	7	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	7	Disattivare l'anteprima automatica dei contenuti dei file.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	8	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	9	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	9	Filtrare il contenuto del traffico web.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	II

8	9	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’amministratore di rete installa e predispone adeguati strumenti hardware/software	II
8	10	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	L’amministratore di rete installa e predispone adeguati strumenti hardware/software	ID
8	11	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.	L’amministratore di rete installa e predispone adeguati strumenti hardware/software	IS

ABSC_ID		Livello	Descrizione	Modalità di implementazione		Tempi
10		1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. Il programma Argo e Nettuno prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola. Il sistema prevede inoltre l'invio automatico a tre indirizzi mail e/o a tre numeri di cellulare, di un messaggio sull'esito dell'esecuzione delle copie. Il sistema di backup Argo e Nettuno prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle. Argo e Nettuno Cloud effettua - Backup del logo delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 8/10 gg		II

10	1	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.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. Per quanto concerne Argo e Nettuno il sistema di backup effettua il salvataggio della base dati. L'installazione dei programmi è possibile in qualsiasi momento dal sito internet di Argo e Nettuno, così come l'eventuale ripristino del motore di database utilizzato (Sybase ver. 8.0.2.4495) Argo e Nettuno Cloud oltre ad esser dotato di un sistema di backup con retention di 8/10gg dei dati ed un sistema di retention di 2/4 gg delle immagini dell'intera infrastruttura e configurato con un sistema di DR Real Time che consente il ripristino di un subset depotenziato dell'infrastruttura madre entro 24/48 ore dal Fault completo del sistema principale garantendo, quindi, la continuità di servizio con uno SLA del 98.98 % circa	IS

10	1	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. Argo e Nettuno consente alle scuole di poter effettuare, nella medesima sessione di copie ed in modo completamente automatico, oltre alla copia sul disco del server, anche una copia su unità fisica esterna e, qualora la scuola abbia acquistato il servizio, anche un backup cloud che garantisce l'assoluta salvaguardia e recuperabilità dei dati. I backup Argo e Nettuno Cloud sono conformi a tutte le regole attuali per il Disaster Recovery	IS
10	2	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. Argo e Nettuno effettua una verifica al termine della creazione del file compresso contenente le copie. La simulazione del ripristino dei dati è comunque buona pratica da adottare con frequenza almeno mensile.	ID
10	3	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.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. Il backup effettuato da Argo e Nettuno è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha generato. Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Argo e Nettuno Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni Argo e Nettuno	II

			Cloud sono cifrate e protette da protocollo HTTPS	
10	4	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.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. Vedi quanto indicato nel punto 10.1.3.A, in particolare è possibile effettuare una copia su un disco esterno, ad esempio, e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server. I backup Argo e Nettuno Cloud sono conformi a tutte le regole attuali per il Disaster Recovery	II

ABSC_ID		Livello	Descrizione	Modalità di implementazione	Tempi
13		1	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'amministratore di rete verifica che i dati siano trattati in conformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	II
13		2	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	L'amministratore di rete verifica che i dati siano trattati in conformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	IS
13		3	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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
13		4	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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
13		5	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.	L'amministratore di rete verifica che i dati siano trattati in conformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	IS

13	5	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.	L'amministratore di rete verifica la presenza di siffatti dispositivi e li include nella lista dei dispositivi autorizzati sulla rete	IS
13	6	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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
13	6	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS

13	7	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software	IS
13	8	Bloccare il traffico da e verso url presenti in una blacklist.	L'amministratore di rete verifica che il firewall in uso sulla rete permetta le gestione di blacklist e whitelist	II
13	9	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.	L'amministratore di rete predispone che i sistemi di copiatura mantengano le regole di controllo sui dati e verifica che i software in uso consentano l'applicazione di tali regole	IS