ISTITUTO ISTRUZIONE SUPERIORE - "M. MORELLI - D. COLAO"-VIBO VALENTIA
Prot. 0009761 del 29/12/2017
C23 (Uscita)

Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO DI ISTRUZIONE SUPERIORE "MORELLI-COLAO"
LICEO GINNASIO STATALE "M. MORELLI"
LICEO ARTISTICO "D. COLAO"
Via XXV APRILE, 1 - VIBO VALENTIA

Cod. meccanografico: VVIS00700G
Cod. fiscale: 96034290799

http://www.iismorellicolao.gov.it/
e-mail: vvis00700g@istruzione.it
pec: vvis00700g@pec.istruzione.it

tel.: 0963/376736
0963/376760

IL DIRIGENTE SCOLASTICO

- VISTO il D.Lgs 165/2001;
- VISTA la circolare AGID n. 2 del 18/04/2017;
- VISTO il D.Lgs 82/2005 (Codice dell'Amministrazione Digitale);
- VISTO il D. Lgs 179/2016;
- VISTA la Nota MIUR n. 3015 del 20/12/2017 avente ad oggetto "Misure minime di sicurezza ICT per le pubbliche amministrazioni";
- VISTA la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 (Misure Minime di Sicurezza ICT Per Le Pubbliche Amministrazioni) in particolare le indicazioni sulle misure minime.

ADOTTA

Le misure minime di sicurezza ICT, al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informatici, ai sensi dell'art. 3 del D. Lgs 82/2005 così come modificato dal Decreto legislativo del 26/08/2016 n. 179.

La rete dell'Istituto d'Istruzione Superiore "Morelli-Colao" di Vibo Valentia è strutturata in due segmenti:

- **segmento della didattica:**
  - rete didattica Liceo Classico (cablata con Wi-Fi)
  - rete di Laboratori Liceo Classico:
    - Lab. Informatica (cablata con Wi-Fi)
    - Lab. Linguistico (cablata con Wi-Fi)
    - Lab. multimediale e videoconferenza (cablata con Wi-Fi)
    - Aula magna (cablata con Wi-Fi)
    - Sala insegnanti (cablata con Wi-Fi)
    - Auditorium-Palestra (cablata con Wi-Fi)
    - Lab. Cl@sse 2.0 (cablata con collegamento Wi-Fi)
    - Lab. Cl@sse 3.0 (cablata con collegamento Wi-Fi)
    - Aule con registro elettronico (Cablate con Wi-Fi)
  - rete d'istituto/didattica Liceo Artistico (cablata con Wi-Fi)
  - rete di Laboratori Liceo Artistico:
    - Lab. Informatica (cablata con Wi-Fi)
    - Lab. Linguistico (cablata con Wi-Fi)
    - Aula Magna (cablata con Wi-Fi)
    - Sala insegnanti (cablata con Wi-Fi)
    - Laboratori artistici (cablati con Wi-Fi)
    - Aule con registro elettronico (Cablate con Wi-Fi)

- **segmento della segreteria**: Servizi di rete client/server per applicativi solo alcuni (magazzino, rilevazione presenze, gestione personale) sono condivisi in modalità client server per la gestione dei dati, l'architettura logica e fisica della rete è peer to peer. Per la gestione Protocollo, Alunni e Registro Elettronico, non sono presenti S.O. e device per la gestione client/server, ma tutti i servizi e dati sono gestiti in cloud.

Il segmento della didattica presenta un rischio molto basso poiché le informazioni che transitano sono solo didattiche, non sono presenti dati sensibili poiché inerenti ricerche e applicativi didattici, senza alcun riferimento a situazioni o persone reali.

La rete di segreteria tratta dati più complessi a rischio medio a tal fine le misure di sicurezza prevedono la separazione logica hardware e software dei due segmenti di rete (didattica e di segreteria). La rete di segreteria e i relativi dispositivi sono dotati di password personalizzate e rispondenti agli standard di sicurezza, è attivo un firewall per tutta la rete che gestisce la segreteria e un antivirus sempre attivo. Per quanto concerne la protezione fisica dei dispositivi, gli stessi sono posizionati in un ambiente fisicamente protetto.

Ogni laboratorio informatico (con ciò si intende la strumentazione informatica di ogni plesso) è affidato ad un responsabile di laboratorio. Ognuna delle postazioni di lavoro della segreteria è affidata ad un operatore con rapporto 1:1 e a gestione esclusiva.

L'intera rete di istituto è protetta dall'esterno da un sistema Firewall (My Security Area di Tim s.p.a. che comprende una serie di servizi di sicurezza ad esso associati) , gli accessi Wi-Fi sono protetti e gestiti da un sistema pfSense, tramite MAC e voucher. La rete di segreteria, a tutela dei dati gestiti, è separata da un Firewall di classe diversa.

Il dirigente è supportato dai responsabili di laboratorio e dagli operatori di segreteria.

Le misure sono descritte nell'allegato 1 "Modulo implementazione - Misure Minime" al quale si rinvia.

In qualità di scuola fruitrice dei servizi web Argo, per quanto riguarda la sicurezza informatica, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository, si rimanda alle informazioni relative al servizio erogato all'istituzione scolastica di cui all'allegato 2 rilasciato da **ARGO SOFTWARE s.r.l..**

Il Dirigente Scolastico
Raffaele Suppa

Il presente documento è firmato tramite firma digitale certificata dal M.I.U.R.

ALLEGATO 1 - Modulo implementazione Misure (Minime – Standard – Avanzate)

SI RITIENE SIANO SUFFICIENTI SOLO LE MISURE LIVELLO M – NOTA MIUR 3015 DEL 20/12/2017

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 è conservato negli uffici di segreteria con accesso a personale autorizzato. L'inventario elenca i dispositivi informatici collegati in rete in modo permanente. Per tutti i device che gestiscono dati sensibili tutelati da privacy si rimanda al disciplinare tecnico sulla sicurezza (196/2003).
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'elenco di cui alla misura 1.1.1 è aggiornato. Le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario. L'aggiornamento dell'elenco è a carico del amministratore di sistema.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Vedi punto 1.1.1. - Le macchine possono essere collegate solo previa registrazione di indirizzo IP o di MAC.

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.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	L'installazione di software è bloccata per tutti gli utenti. Eventuali nuovi software sono installati esclusivamente dall'amministratore di sistema dopo verifica della tipologia e della funzionalità. L'inventario è conservato. L'inventario contiene: • tipologia dispositivo • nome del software • fornitore e/o marca • versione • soggetto autorizzante • eventuale data di scadenza dell'autorizzazione L'aggiornamento dell'elenco dei software è a carico dell'amministratore. Sono state date direttive al personale ed all'amministratore di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata all'Amministratore di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono stati concessi solamente all'amministratore di sistema (vedi 5.1.1)

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.	Premettendo che su ciascun Personal Computer, a cui gli allievi accedono con l’utenza assegnata alla propria classe abilitata ad effettuare operazioni ristrette (l’installazione di software non è contemplata), il responsabile esegue ricognizioni periodiche per la verifica del software installato su ciascun dispositivo e comparano il risultato con l’elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell’elenco viene immediatamente disinstallato. Tutti i dispositivi sono protetti con account limitato ed antivirus.
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.	Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica. Per la rete di segreteria tutte le macchine sono protette da password e hanno un antivirus installato per la navigazione in rete. Gli utenti non hanno privilegi di amministratore. Eventuali danni sui S.O. vengono risolti attraverso l'operazione di ripristino del sistema.
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 all'organizzazione.	Vedi 3.1.1. Le macchine omogenee per tipo e sistema operativo hanno delle configurazioni standardizzate.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sono state date disposizioni ai responsabili di laboratorio in tale senso. Il sistema provvede automaticamente al ripristino della configurazione in caso di alterazioni.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Non si ritiene necessario attivare immagini di ripristino poiché per i laboratori didattici lo stesso può avvenire mediante un ripristino totale del sistema, tanto perché non esistono dati da preservare nel tempo. La rete di segreteria opera con software proprietari e database delocalizzati rispetto ai quali non è necessaria l'immagine in quanto l'eventuale ripristino da crash è facilmente riparabile mediante l'intervento delle aziende fornitrici. I dati invece sono oggetto di backup ricorrenti a cadenza giornaliera.

3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	La rete didattica è separata da quella della segreteria. Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…). Le operazioni di amministrazione da remoto sono impedite. In caso di necessità vengono abilitate temporaneamente connessioni attraverso protocolli sicuri e disabilitate al termine dell'intervento.
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.	In caso di modifiche si procede alla riconfigurazione dei firewall e ad una scansione completa dei sistemi. Per la segreteria si utilizza il software antivirus e la protezione firewall posta anche all'ingresso della rete. Per la didattica non sono necessari software specifici. I responsabili di laboratorio e gli operatori di segreteria sono 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	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common ConfigurationEnumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Gli antivirus sono configurati per l'aggiornamento automatico. Sono state date disposizioni agli operatori di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle 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.	I dispositivi sono configurati per l'aggiornamento automatico del S.O. L'applicazione delle patch di vulnerabilità è schedulata dai responsabili di laboratorio e dagli operatori di segreteria. Qualora l'applicazione automatica delle patch non abbia avuto successo o provochi gravi problemi al funzionamento dei sistemi, sarà necessario bloccare l'attività di patching.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non esistono dispositivi air-gapped.
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.	Sono state date disposizioni ai responsabili di laboratori e agli operatori di segreteria di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie saranno attivate le eventuali contromisure
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.).	E' stato redatto il DPP (Documento Programmatico in materia di Privacy) per la gestione del rischio informatico in generale. Si analizzano le azioni suggerite dal report prodotto dello strumento di scansione, agendo in base alle priorità ivi indicate.
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 4.8.1 Sono state date disposizioni agli operatori di segreteria e ai responsabili di laboratorio. Tutte le patch relative a vulnerabilità vengono immediatamente implementate appena disponibili.
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.	La rete didattica è strutturata in modalità peer to peer ogni pc ha più account, i privilegi di amministrazione sono riservati ai soli tecnici. La rete di segreteria è di tipo peer to peer e ogni utente ha i privilegi di amministratore ciò si rende necessario per la gestione e il controllo completo dei software, degli aggiornamenti e delle minacce.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Non è necessario registrare gli accessi nella rete di segreteria poiché vi è un rapporto 1:1 tra operatore e dispositivo. La rete didattica non presenta tale necessità.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I documenti di nomina dei responsabili di laboratorio e degli assistenti amministrativi sono consegnati agli stessi e una copia è conservata in segreteria. Vedi anche Disciplinare Tecnico per la Sicurezza
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.	Le credenziali vengono sostituite prima dell'allacciamento in rete. Agli operatori sono state impartite adeguate istruzioni al riguardo.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	

5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	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"
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password trimestrale o semestrale in base al grado di criticità.
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 password precedentemente utilizzate.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Agli operatori di segreteria e ai responsabili di laboratorio sono state 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, tuttavia, ove possibile si crea un account per ogni alunno/classe.
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.	Agli operatori di segreteria e ai responsabili di laboratorio sono state impartite adeguate istruzioni al riguardo.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali vengono raccolte in busta chiusa e conservate dal responsabile del trattamento. L'elenco cartaceo delle PWD è custodito in cassaforte ed accessibili solo al responsabile della struttura ed al direttore sga. Le credenziali di accesso sono personali e quindi non possono essere conosciute e/o archiviate.
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. I certificati digitali in possesso al Dirigente scolastico sono custoditi 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.	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico. Risulta inoltre presente software per il rilievo della presenza di malicious software (Malwarebytes Anti-Malware) con settaggio per l'aggiornamento automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC, portatili e server Windows è attivato un firewall.
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.	È stata data disposizione di inibire l'uso di dispositivi esterni a quelli necessari per le attività di segreteria. Ciò non è possibile per la rete didattica che per sua natura non può essere limitata ma deve essere estesa anche ai dispositivi personali degli alunni con accesso controllato tramite Mac o voucher.
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 ExecutionPrevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	

8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Nella segreteria è inibito l'uso di dispositivi removibili vista la presenza della rete interna. Ogni postazione è protetta da password. E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro. Per la didattica è inibito l'uso di dispositivi mobili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	E' stata data disposizione agli di segreteria di configurare in tal senso le postazioni di lavoro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Tutte le postazioni sono configurate per l'esecuzione automatica di scansione anti-malware. E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
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), un server proprio e i servizi Educational di Google che include il filtraggio richiesto.
8	9	2	M	Filtrare il contenuto del traffico web.	L'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso.
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'account di posta elettronica ministeriale blocca i file non necessari. L'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	I software che gestiscono dati da proteggere richiedono automaticamente le copie di backup pena il blocco delle funzioni.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Si attivano ricorrenti punti di ripristino per il S.O. Per il resto si veda punto 10.1.1.
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.	È stata data disposizione agli uffici per effettuare una copia di backup su dispositivi protetti, inacessibili da personale non autorizzato e non permanentemente accessibili dal sistema.

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 e segnatamente quelli ai quali va applicata la protezione crittografica	I dati gestiti dalla scuola non contengono protezione crittografica. I servizi erogati in rete dai fornitori tramite la loro infrastruttura tecnologica, ospitanti dati dell'istituzione scolastica sono gestiti su cloud garantito dai fornitori di servizi (ARGO). È stata richiesta ai fornitori la dichiarazione relativa alle misure implementate
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 LossPrevention) 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.	Vedi misura 8.9.2 L’antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso. La misura è implementata nella configurazione del browser.
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.	

ARGO SOFTWARE s.r.l.
P.IVA 00838520880
Zona Ind. III fase, 97100-Ragusa
Ass.: 0932-666412 Amm. 0932-667550
Fax: 0932-667551
e-mail: info@argosoft.it WEB: http://www.argosoft.it

Policy Argo Software
in materia di protezione e disponibilità dei dati relativi ai servizi web

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza informatica, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web argo.

La Argo software srl è impegnata costantemente a migliorare l'efficacia e l'efficienza dei propri processi di gestione dei dati e dei servizi web offerti alle scuole, nell'ottica della salvaguardia dell'integrità dei dati, della disponibilità delle informazioni stesse in tempi adeguati e della continuità operativa dei servizi.

Nell'ambito della continuità operativa, Argo Software, adotta tutti gli accorgimenti organizzativi, le soluzioni tecniche e procedurali idonee al ripristino delle condizioni di funzionamento e di operatività antecedenti ad eventuali eventi disastrosi ed è impegnata, con continuità, ad adottare tutte le misure di sicurezza che trovano fondamento e riferimento all'interno del quadro normativo italiano (Codice della Privacy, Linee guida AgID per il Disaster Recovery, Circolare AgID nr. 2/2017 sulle misure minime di sicurezza ICT per le PP.AA.).

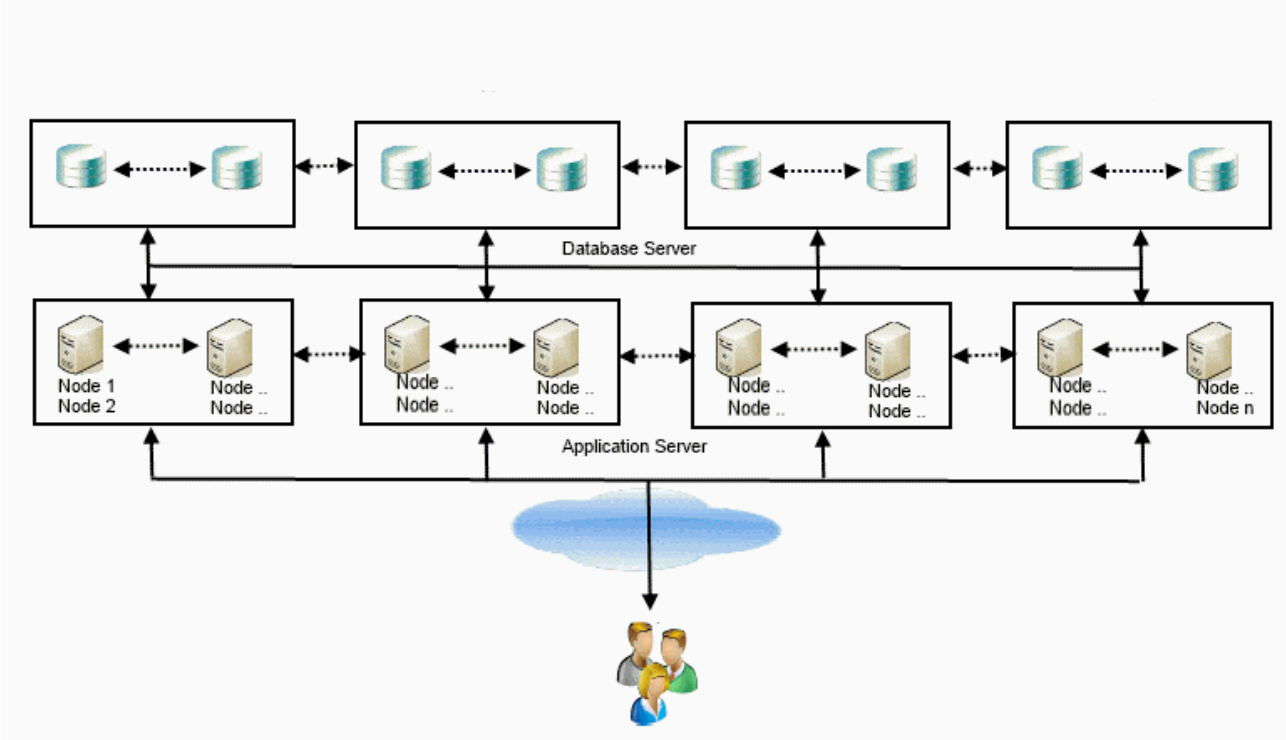
Tipologia dei dati gestiti dalla Argo Software

I dati gestiti dalla Argo Software riguardano la profilazione degli utenti fruitori dei servizi web Argo e i dati contenuti negli archivi delle scuole fruitrici dei medesimi servizi.

In riferimento a quest'ultimi, la natura dei dati varia in base alle caratteristiche del servizio attivato dalla scuola.

Architettura del sistema informatico

Il grafico che segue raffigura l'architettura del sistema informatico adottato dalla Argo Software per la gestione dei servizi web offerti alle scuole.



Le applicazioni, i dati in produzione e i backup risiedono presso datacenter dislocati in diversi siti geografici, all'interno dell'Unione Europea, posti a grande distanza gli uni dagli altri, al fine di fornire maggiori garanzie di protezione in caso di calamità naturali.

Ogni infrastruttura è costituita da una batteria di application e database server.

La gestione e configurazione dei server è eseguita esclusivamente da personale Argo.

La configurazione dei nuovi server è eseguita con procedure semi-automatiche e controllate.

Gli addetti alla gestione dei server sono nominati amministratori di sistema.

Gli accessi ai server e ai servizi di gestione degli stessi sono monitorati. L'accesso da parte degli amministratori viene eseguito sempre attraverso utenze di dominio.

Con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori di sistema da parte del responsabile della gestione privacy Argo.

I log delle operazioni e degli accessi sono marcati temporalmente e archiviati per un periodo di 18 mesi.

Modalità di gestione dei dati e di erogazione del servizio

Il sistema di gestione dei servizi e dei dati adottato da Argo è improntato a criteri di ridondanza dei sistemi informatici e di replicazione dei dati al fine di preservare i clienti da rischi di interruzione prolungata dei servizi e/o di perdita dei dati.

A tal fine ogni infrastruttura Argo è configurata per essere agevolmente convertita da sussidiaria a primaria e viceversa, e i database vengono replicati, in maniera asincrona con un delay ridotto ai tempi necessari alla trasmissione delle transazioni, presso i server delle altre infrastrutture (replicazione speculare dei dati).

Vengono effettuate copie dei database più volte al giorno, a intervalli regolari, e con modalità differenti (full e incrementali).
Le copie full vengono mantenute presso i server delle infrastrutture per sette giorni. Quotidianamente una copia dei dati viene riversata in un sistema di storage, dove viene mantenuta per 2 mesi. Delle suddette copie, una copia settimanale viene mantenuta per un ulteriore periodo di 2 mesi, mentre una copia mensile viene mantenuta per un periodo complessivo di 6 mesi.

L'integrità delle copie di sicurezza nell'operazione di trasmissione verso il sistema di storage è garantita da un sistema di hashing che controlla l'impronta del file di destinazione con quello di origine.

Con cadenza mensile, vengono effettuate prove di ripristino dei backup.

Per i servizi di gestione documentale, è stato implementato un servizio di controllo di integrità dei file che con cadenza mensile verifica gli hash dei file archiviati nel sistema.

Le copie degli applicativi vengono fatte ad ogni aggiornamento e mantenute presso i server dell'infrastruttura primaria.

La Argo è inoltre dotata di uno strumento di monitoraggio continuo degli applicativi web che fornisce in tempo reale, indicatori sulle prestazioni degli stessi, inclusi eventuali picchi di carico.

Procedure di verifica del sistema di protezione dei dati

La Argo Software, oltre ad essersi dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati, ha affidato ad una azienda

specializzata nel settore della sicurezza informatica i servizi di Vulnerability Assessment e Penetration Test.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware si affida esclusivamente a server farm di comprovata affidabilità ed esperienza in materia di sicurezza informatica, e comunque previa verifica delle misure fisiche, logiche e organizzative poste in capo alle infrastrutture informatiche fornite.

Ad ogni fornitore è richiesta come requisito la certificazione ISO 27001 e uno SLA di connettività di almeno il 95% su base annua e una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

I dati viaggiono sulla rete criptati, secondo il protocollo SSL che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche.

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interna dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.

Risoluzione dei contratti di assistenza e fruibilità dei dati

In caso di risoluzione del contratto di assistenza da parte della scuola di un servizio web Argo, la Argo Software garantisce l'accesso ai dati e la fruizione del servizio da parte dell'utente per un ulteriore periodo di un mese dalla data di risoluzione e il mantenimento dei dati per un ulteriore periodo di sei mesi, al termine del quale i dati vengono definitivamente rimossi dai server di produzione.

La scuola può comunque richiedere la cancellazione dei dati prima del termine prestabilito.

Alla risoluzione del rapporto, su richiesta del Dirigente scolastico, una copia dei dati viene fornita alla scuola in formato aperto.

La suddetta procedura si applica anche ai dati e ai documenti relativi ai servizi di gestione documentale Albo Pretorio, Amministrazione Trasparente e Gecodoc

Rispetto normativa privacy

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 29 del D.Lgs. n° 196 del 30 giugno 2003 e successive disposizioni.

Piano di miglioramento

La Argo Software si è posta come obiettivo principale l'implementazione per i suoi asset strategici di un sistema di gestione di sicurezza delle informazioni conforme alla norma ISO 27001.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative.

Ultimo aggiornamento 19/12//2017