MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSIA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO DI ISTRUZIONE SUPERIORE "C. BARONIO"
03039 S O R A (FR) **Ambito 19**

SEDE: Viale San Domenico, s.n.c **Tel.**(0776/ 831284 **Fax** 0776/824594
e-mail: fris027009@istruzione.it **pec:** fris027009@pec.istruzione.it **Codice Fiscale** 91026720606
Web: http://www.iisbaronio.gov.it/ **Cod. Amm.ne: UF2MVR** **Codice Istituto**: **FRIS027009**

(LIVELLO MINIMO – STANDARD E AVANZATO)

Prot. N. vedi segnatura 28/12/2017

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" nella quale viene esplicitamente segnalato che per gli istituti scolastici è sufficiente la verifica del livello "M" .
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.
VISTO l'incarico assegnato alla Fusion Technology srl di redigere il disciplinare tecnico in materia di misure minime di sicurezza stabilito dal D.L.vo N. 196 del 30/06/2003. Società a cui è stato dato l'incarico come amministratore di sistema e che e si impegna ad adottare tutte le misure minime necessarie all'attuazione delle norme della privacy e a quelle della circolare dell'agid N. 2 DEL 18/04/2017confermate dalla nota del miur 3015 del 20/12/2017l .

ADOTTA

Art.1

- Adozione misure minime di sicurezza ICT per le pubbliche amministrazioni -

le **misure minime** (SOLO **MINIME** ESCLUSO **STANDARD** O **AVANZATE** A CARICO SOLO DEI FORNITORI DI SOFTWARE) 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 82/2015.

Art. 2

-Struttura e architettura della rete-

La rete dell'IC/IS "_Cesare Baronio _" di Sora (FR) è strutturata in due segmenti:

- **Segmento della segreteria** con il trattamento dati con connessione via cavo.
- Dati contenuti in **file** immediatamente leggibili ed archiviabili di tipo office microsoft o in altri formati direttamente leggibili tramite applicativi (word excel, power point, acrobat, out look ecc…); il cui accesso è effettuato tramite sistema client/server con tecnologia microsoft, utilizzando la rete dati via cavo esistente nella scuola.
- Dati contenuti in **database** INSTALLATI SU SISTEMI client/server o su workstation il cui inserimento e lettura sono supportati da un applicativo di tipo gestionale installato per alcuni moduli su client server sulla rete locale o workstation e in alcuni moduli in remoto tramite piattaforma cloud fornita dal produttore di software alla cui connessione si accede tramite web.
- Dati inseriti su piattaforme web **messe a disposizione dagli enti preposti** tramite importazione massiva o inserimento manuale (SIDI SOGEI ECC)**.**
- **Segmento della didattica**, con trattamento dati riguardo il registro elettronico con connessioni via cavo o via wi fi e utilizzo della rete dati per fini didattici, non avendo risorse economiche non sono attivate attività di monitoraggio e controllo accessi e filtri dei contenuti adeguati alle esigenze.

Art.3

-Valutazione del rischio, misure di prevenzione e rinvio-

La rete di segreteria tratta dati complessi a rischio medio a tal fine le misure di sicurezza prevedono la separazione tramite firewall 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 e un antivirus. Per quanto concerne la protezione fisica dei dispositivi, gli stessi sono posizionati in un ambiente fisicamente protetto.
Ognuna delle postazioni di lavoro della segreteria è affidata ad un operatore con rapporto 1:1 a gestione esclusiva con possibilità di utilizzo di un altro utente con il suo nome e password .
Il segmento della rete didattica presenta un rischio molto basso poiché le informazioni che transitano oltre alla connessione web per il registro elettronico sono solo didattiche, non sono presenti dati sensibili poiché inerenti a ricerche e applicativi didattici, senza alcun riferimento a situazioni o persone reali.
Il dirigente è supportato dai responsabili di laboratorio, dagli animatori digitali e dagli operatori di segreteria.

Le misure sono descritte nell'allegato 1"*Modulo implementazione Misure **Minime** (**Standard o Avanzato ove interessati**) con suggerimenti"* al quale si rinvia.

Il Dirigente Scolastico

__Prof.ssa Biancamaria Valeri
(firmato digitalmente)
(marcatura temporale o conservazione a norma)

ALLEGATO 1 - Modulo implementazione Misure (Minime – Standard Avanzate per i fornitori di software)

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 delle risorse di segreteria è riportato in allegato "B" Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003 e viene implementato entro il 31 marzo di ogni anno con un file xls. L'inventario elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio ed è strutturato nel modo seguente: • *Tipo di apparato e codice identificativo assegnato* • *Descrizione breve del tipo di dispositivo;* • *indirizzo IP;* • *Collocazione dell'apparato* • *Persona alla quale è assegnato in caso di client.* Verrà implementato con la stessa metodologia anche un elenco dei dispositivi collegati alla didattica, come le risorse economiche o interne lo permetteranno.
1	**3**	**1**	**M**	**Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.**	L'elenco delle risorse di cui alla misura 1.1.1 è aggiornato quando saranno aggiunte nuove risorse , con verifica annuale con il disciplinare tecnico. Verrà implementato con la stessa metodologia l'aggiornamento dell'elenco dei dispositivi collegati alla didattica, come le risorse economiche o interne lo permetteranno.
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.

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'inventario dei software di segreteria è riportato nel Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003 e viene implementato entro il 31 marzo di ogni anno. . L'inventario contiene: • *Nome del software* • *Fornitore e/o marca* • *Versione del software* • *Dove è installato il software* • *Dove sono archiviati i dati prodotti dal software.* • *Sistemi di copia di dati prodotti dal software.* Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori 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 agli amministratori di sistema (vedi 5.1.1). Verrà implementato con la stessa metodologia l'aggiornamento dell'elenco dei software collegati alla didattica, come le risorse economiche o interne lo permetteranno.
2	**3**	**1**	**M**	**Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.**	Nelle macchine di segreteria nessun utente ha l'abilitazione per installare nuovi software. Le scansioni vengono effettuate dai responsabili della sicurezza del sistema informatico. Per la didattica vista la sua natura didattica non sono attivi sistemi di scansione e la gestione viene attualmente lasciata ai docenti ed ai responsabili di laboratorio.

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 si prevede oltre a quanto detto al punto precedente un antivirus per la navigazione in rete. Sono utilizzate copie immagine conservate come descritto al punto 3.3.1 e 3.3.2. Verrà implementato con la stessa metodologia l'aggiornamento delle configurazioni dei dispositivi collegati alla didattica, come le risorse economiche o interne lo permetteranno.
3	**2**	**1**	**M**	**Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.**	Vedi 3.1.1.
3	**2**	**2**	**M**	**Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.**	Sono previste dal Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003 sistemi di backup e ripristino dati sia per i server che per i client della segreteria. Per la parte didattica la gestione viene attualmente lasciata ai docenti ed ai responsabili di laboratorio.
3	**3**	**1**	**M**	**Le immagini d'installazione devono essere memorizzate offline.**	La rete di segreteria opera con software proprietari con in parte applicativi e dati delocalizzati e pertanto è a cura del fornitore di software la creazione di immagini di ripristino. A riguardo i dati su server in locale il sistema di ripristino è delocalizzato e non è necessaria l'immagine in quanto l'eventuale ripristino da crash è facilmente riparabile mediante l'intervento delle aziende fornitrici. Per le immagini dei server e dei client sono perviste dal Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003. Sono sistemi di backup e ripristino d'installazione sia per i server che per i client della segreteria. Per la didattica attualmente non si ritiene necessario implementare un sistema di memorizzazioni immagine.

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…) Tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri.

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.**	Per la segreteria si utilizza il software antivirus in aggiunta al software di scansione vulnerabilità tipo SECPOD SANER. 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	**4**	**1**	**M**	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**	Sono state date disposizioni agli operatori di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	L'applicazione delle patch di vulnerabilità per la segreteria è a carico dell'amministratore di sistema per la didattica è a carico degli animatori digitali e dei responsabili di laboratorio. In quest'ultimo caso 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 e far intervenire personale adeguatamente preparato per la soluzione.
4	**5**	**2**	**M**	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.**	I dispositivi air-gapped sono connessi solo nella rete didattica essendo la rete wi-fi di segreteria bloccata.
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 contattare l'amministratore di sistema per la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie saranno attivate le

					eventuali contromisure
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 DPS (*Documento Programmatico in materia di Privacy)* per la gestione del rischio informatico in generale. Si analizzano le azioni suggerite dal report prodotto dalla dalla redazione del documento, informando gli organi competenti delle risorse economiche necessarie ed agendo in base alle priorità ivi indicate in base alle disponibilità economiche.
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.

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 di segreteria è di tipo client/server ogni utente ha i privilegi di amministratore per la gestione e il controllo completo del software, e degli antivirus impedendo la limitazione dei privilegi.
5	**1**	**2**	**M**	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**	Gli accessi sono controllati dal server di dominio basato su tecnologia client server microsoft con utente e password registrando ogni accesso effettuato.
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.
5	**3**	**1**	**M**	**Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.**	Agli operatori sono state impartite adeguate istruzioni al riguardo.
5	**7**	**1**	**M**	**Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).**	Sono fornite indicazioni a tutti gli utenti per l'utilizzo di password di autenticazioni "forti", "almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola"
5	**7**	**3**	**M**	**Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)**	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi. Misura che, in realtà, è già prevista obbligatoriamente dall'allegato B "Misure minime" del Codice Privacy

5	**7**	**4**	**M**	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	Sono fornite indicazioni a tutti gli utenti per impedire il riutilizzo delle ultime 6 password.
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.**	Le utenze amministrative anonime saranno utilizzate solo per situazioni di emergenza dagli amministratori di sistema.
5	**11**	**1**	**M**	**Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.**	Già previsto nella Privacy, vengono raccolte in busta chiusa e conservate dal responsabile del trattamento in un luogo sicuro.
5	**11**	**2**	**M**	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	Non si utilizzano certificati digitali per l'autenticazione delle utenze di amministrazione se non quelle di sistema.

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 della segreteria è installato un antivirus con aggiornamento automatico di varie tipologie secondo le disponibilità economiche della scuola.
8	**1**	**2**	**M**	**Installare su tutti i dispositivi firewall ed IPS personali.**	Su tutti i PC, portatili e server Windows è attivato il firewall di Windows oltre al firewall su centro stella.
8	**3**	**1**	**M**	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**	Nel disciplinare dei dipendenti è stata data disposizione di limitare 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.
8	**7**	**1**	**M**	**Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.**	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
8	**7**	**2**	**M**	**Disattivare l'esecuzione automatica dei contenuti dinamici**	E' stata data disposizione agli operatori di segreteria di configurare

				(e.g. macro) presenti nei file.	in tal senso le postazioni di lavoro salvo problemi di operatività su alcuni applicativi utilizzati dalla segreteria.
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.**	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) 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'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso.

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 sistemi di copia di sicurezza sono riportati nel Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003 e viene implementato entro il 31 marzo di ogni anno. Vengono valutati anche il disaster recovery ed i tempi di ripristino del sistema.
10	**3**	**1**	**M**	**Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.**	Sistemi di riservatezza delle informazioni sono riportati nel Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003 e viene implementato entro il 31 marzo di ogni anno.
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.**	L'accesso ai supporti di copie sono riportati nel Disciplinare Tecnico per le misure minime sicurezza D.Lgs 196/2003 e viene implementato entro il 31 marzo di ogni anno.

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 segnatamente quelli ai quali va applicata la protezione crittografica**	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è fisicamente controllato e protetto da password e dal profilo utente. Per la didattica vista la sua natura didattica non sono attivi sistemi di scansione e la gestione viene attualmente lasciata ai docenti ed ai responsabili di laboratorio.
13	**8**	**1**	**M**	**Bloccare il traffico da e verso url presenti in una blacklist.**	Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall. Per la didattica vista la sua natura didattica non sono attivi sistemi di scansione e la gestione viene attualmente lasciata ai docenti ed ai responsabili di laboratorio.