Istituto Professionale di Stato "Alfredo Beltrame"
Servizi per l'enogastronomia e l'ospitalità alberghiera
Via Carso, 114 - 31029 Vittorio Veneto (TV)
☏ 0438/556367 - 556128 - 556060 🖷 0438/946336
✉ beltrame@alberghierobeltrame.gov.it; http://www.alberghierobeltrame.gov.it
C.F. 93005790261

Spettabile
Sig Paladino Giuseppe

Vittorio Veneto, 16.02.2016

OGGETTO: Nomina ad Amministratore di sistema

Egregio Signor Paladino Giuseppe,
come previsto del provvedimenti del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", il titolare del trattamento I.P.S.S.A.R. "Alfredo BELTRAME", legalmente rappresentato dal Dirigente Scolastico, valutate le sue caratteristiche soggettive di esperienza, capacità e affidabilità, le attribuisce l'incarico di **Amministratore di Sistema**. Nello svolgimento delle sue funzioni potrà avvalersi del supporto tecnico di società – professionisti esterni, nominati responsabili esterni del trattamento da parte dell'Istituto.

In qualità di amministratori di sistema avrà il compito di :

-generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate e secondo aggiornati criteri tecnici e di sicurezza, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dei dati personali;
-adottare programmi antivirus, firewall, ed altri strumenti sia software che hardware, che garantiscano - anche in base alle conoscenze tecniche acquisite in base al progresso tecnico - la sicurezza nel trattamento dei dati personali secondo i criteri generali stabiliti dall'art. 31 del d.lgs 196/03 e dalle previsioni contenute nell'allegato B e negli articoli 33-36 del decreto stesso;
-controllare periodicamente l'efficienza dei sistemi tecnici, comunque adottati, per verificarne la validità, anche secondo consolidati criteri tecnici di valutazione;
-redigere un apposito verbale che dovrà contenere l'indicazione di coloro che vi hanno partecipato, le modalità di controllo effettuato ed altresì gli strumenti - di qualsiasi natura - utilizzati per provvedervi, i risultati ottenuti ed eventualmente gli ulteriori accorgimenti da adottare onde implementare la sicurezza del trattamento;
-qualora terzi esterni intervengano sugli elaboratori vigilare al fine di impedire il trattamento dei dati in essi contenuti;
- vigilare - secondo le prassi istituite ed in accordo con gli altri collaboratori del titolare - che gli individuati incaricati al trattamento dei dati personali si attengano alle procedure di volta in volta indicate specificamente, sia oralmente che per iscritto, anche in ordine alla custodia e segretezza della parola chiave (e/o dei codici identificativi) loro assegnata ed altresì in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza nel trattamento;
-collaborare alla redazione annuale della parte del documento programmatico sulla sicurezza relativa a tutta l'attività logica di trattamento dei dati che si svolge mediante reti di elaboratori o terminali sia accessibili che non accessibili al pubblico attraverso reti di telecomunicazioni ed assistere il titolare e il responsabile del trattamento nella individuazione degli altri criteri di sicurezza da adottare sia organizzativi che fisici**;**
-individuare, unitamente al titolare e/o al responsabile del trattamento dei dati, le modalità e le procedure di reimpiego dei supporti di memorizzazione logica ex allegato D d.lgs 196/03 e, se del caso, individuare gli strumenti e le procedure adeguate per procedere alla distruzione e smaltimento dei supporti di memorizzazione che non possono essere riutilizzati;
-redigere unitamente al titolare e/o responsabile del trattamento un apposito verbale in cui siano indicati i supporti che possono essere reimpiegati e /o distrutti, le modalità tecniche adottate sia nel caso di reimpiego che di distruzione e le persone alle quali dette incombenze siano affidate;

Si allega a far parte del documento l'allegato B in cui oltre alle istruzioni vi sono ulteriori compiti dell'amministratore.

Allegato B - ISTRUZIONI E COMPITI DELL'AMMINISTRATORE DI SISTEMA

Codice in materia di protezione dei dati personali
B. Disciplinare tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza
19. [soppresso]

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. [soppresso] ([1])

Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

VADEMECUM PER AMMINISTRATORE DI SISTEMA

Il nuovo testo unico esige che tutte le aziende adottino delle misure almeno minime di sicurezza, per il trattamento in elaboratori elettronici. Pertanto qui di seguito diamo le indicazioni previste dalla legge.
1) Ogni incaricato dev'essere dotato di user name e password univoci e personali (le credenziali di autenticazione);
2) Le suddette credenziali devono essere disattivabili dopo sei mesi di inutilizzo;
3) La password dev'essere cambiata almeno ogni sei mesi e ogni tre per i dati sensibili e giudiziari (ufficio del personale);
4) La password deve avere un minimo di otto caratteri (o il massimo dei caratteri consentiti dal sistema), non dev'essere riconducibile alla persona;
5) E'necessario adottare dei sistemi anti intrusivi, e al loro periodico aggiornamento, annotare l'aggiornamento stesso in apposito registro;
6) E'necessario effettuare un back up dei dati con cadenza almeno settimanale;
7) E'necessario predisporre un sistema che permetta all' utente di non rendere accessibile ad altri i dati aperti con la su credenziale. Per evitare blocchi del lavoro consigliamo l'attivazione degli screen server. L'amministratore di sistema deve altresì predisporre la parte tecnica del documento programmatico per la sicurezza. In questo deve:

- Redarre un elenco dei rischi informatici analizzando la tipologia di rischio dell'azienda (es. rischi esterni- basso);
- Indicare le misure da adottare per garantire l'integrità e la disponibilità dei dati;
- Descrivere i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- Indicare i software adottati dall' azienda;
- Descrivere il sistema di sicurezza dell'azienda;
- Descrivere le modalità e i tempi del back up;
- Indicare i criteri che hanno spinto a scegliere un sistema piuttosto che un altro.

Firma Del Titolare Del Trattamento
Dirigente Scolastico

_____

Firma Dell'amministratore Di Sistema

_____

ALLEGATO: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 - (G.U. n. 300 del 24 dicembre 2008)

(così modificato in base al provvedimento del 25 giugno 2009)