the net (r)evolution

netatwork

Linee guida per l'utilizzo e la gestione del S.I. del Liceo Darwin

Scopo di questo documento è descrivere in breve il Sistema Informativo del Liceo Darwin, e le misure da adottare per una corretta gestione dello stesso oltre a indicare quali sono gli adempimenti che gli amministratori di sistema sono tenuti a espletare nel corso delle attività di gestione del sistema. Il documento illustra inoltre quali siano le norme generali di utilizzo degli strumenti informatici a disposizione del personale, dei docenti e degli allievi.

Descrizione della rete e delle dotazioni hardware e software

La rete informatica del Liceo Darwin è costituita da un parco hardware di 3 server basati su Windows 2008 Server R2 (Srv-Darwin, Srv-Labs, Srv-Main) con tecnologia Raid e quasi 200 client compatibili basati su piattaforma Windows XP, Windows 7 suddivisi tra 25 PC, 42 NComputing, 90 Netbook distribuiti tra gli uffici della Segreteria e della Presidenza, nei quali avviene il trattamento dei dati, e i vari locali adibiti alle attività scolastiche, oltre a 34 iPad distribuiti tra studenti e docenti della classe 2.0. Attraverso la configurazione di un switch HP Procurve 2924al è stato possibile implementare delle Vlan (Virtual Lan) in modo da suddividere la rete in quattro segmenti distinti:

Vlan 1 : Servers
Vlan 2 : Segreteria
Vlan 3 : Laboratori
Vlan 4 : Wireless (nuova implementazione)

Attraverso tale configurazione sono state definite delle politiche di comunicazione tra le varie Vlan al fine di garantire la sicurezza e la riservatezza di dati sensibili e identificativi.

Sulla rete vengono implementate delle politiche di backup dei dati basate su disco con frequenza giornaliera, settimanale e mensile.

Le operazioni di ripristino dei dati vengono eseguite dagli amministratori di sistema su richiesta dell'amministrazione.

netatwork

Principi di carattere generale

- I trattamenti di dati personali effettuati all'interno dell'Istituzione Scolastica devono avvenire secondo le modalità definite dalla normativa vigente.
- Occorre custodire e controllare i dati personali oggetto del trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dai casi consentiti o altrimenti trattati in modo illecito.
- Chiunque, all'interno di questa istituzione scolastica, tratti dati personali, è tenuto all'obbligo della dovuta riservatezza in ordine alle informazioni delle quali sia venuto a conoscenza.
- L'obbligo di mantenere la dovuta riservatezza, in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, permane anche quando sia venuto meno l'incarico stesso.
- Tutti i trattamenti dei dati personali vanno necessariamente organizzati secondo una procedura che garantisca: una continua e idonea custodia dei dati oggetto del trattamento; un adeguato controllo sugli accessi non autorizzati ai dati; il maggior livello possibile di sicurezza in merito alla conservazione dei dati.
- Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola. **Al di fuori delle finalità strettamente istituzionali, dentro la scuola non si possono trattare dati personali né su supporto cartaceo né su supporto elettronico.**
- **I dati personali oggetto dei trattamenti devono essere esatti ed aggiornati, inoltre devono essere pertinenti rispetto alle finalità del trattamento, completi e non eccedenti le finalità per le quali vengono raccolti e trattati. Ne consegue che i trattamenti dei dati vanno ridotti a quanto indispensabile rispetto alle finalità istituzionali perseguite.**
- Nell'ambito delle indicazioni del presente documento, particolare attenzione va prestata al trattamento di dati sensibili e giudiziari.
- L'istituto esegue verifiche periodiche sull'attualità degli incarichi affidati in merito al trattamento dei dati, nonché sull'esattezza e l'aggiornamento dei dati sensibili e giudiziari, sulla loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite.

netatwork

Descrizione delle politiche di sicurezza implementate

- Per evitare l'accesso non autorizzato alle postazioni personal computer sono state inserite password all'avvio di ogni terminale.
- Per evitare accessi non autorizzati al sistema operativo delle postazioni, ogni unità del personale è dotata di un proprio username e password (con scadenze semestrali, costituite da 8 caratteri alfanumerici per contrastare gli attacchi alle password basati su dizionari). Per gli studenti viene invece implementata una user/pwd per ogni classe.
- Per evitare accessi non autorizzati ai dati custoditi sui server, sono state inserite delle policy di controllo e di accesso ai file, applicate a gruppi di utenti con comuni mansioni e responsabilità.
- Sono previste politiche di salvataggio e ripristino dei dati per minimizzare il rischio di perdita di quest'ultimi
- Sulla rete è in esecuzione un prodotto Antivirus (Trend Micro) gestito centralmente su un server, oltre a ulteriori prodotti antivirus freeware
- Per evitare l'accesso non autorizzato alla rete informatica dall'esterno è stato installato un firewall con funzionalità di filtro dei contenuti Web, atto a contrastare minacce per la sicurezza informatica e l'utilizzo improprio di Internet (categorie di siti non inerenti all'attività didattica).
- I sistemi di rete sono sottoposti a monitoraggio preventivo al fine di prevenire problematiche critiche che possano dare origine a crash di sistema.

Norme generali per gli utenti relativi all'utilizzo di PC, Tablet e Smartphone all'interno della rete informatica del Liceo Darwin

- **L'utlizzo dei PC, Tablet e/o Smartphone e della Rete interna ed esterna è permesso esclusivamente per lo svolgimento delle attività istituzionali della scuola;**
- Per l'accesso in modalità wireless da parte degli Smartphone/Tablet è previsto un sistema di autenticazione basato su Radius, tale per cui solo chi è in possesso di uno username e password accreditati presso il sistema informativo del Liceo, può accedere ad Internet e alle basi dati.

- **E' fatto divieto, agli utilizzatori di strumenti elettronici, di lasciare incustodito, o accessibile lo strumento elettronico stesso;** in particolare, in caso di allontanamento anche temporaneo dal posto di lavoro, è vietato lasciare aperto il proprio sistema operativo con la password inserita, a meno che il sistema non richieda automaticamente la password in caso di inattività prolungata;
- L'accesso ai dati trattati elettronicamente da parte degli incaricati e degli addetti esterni alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- Tutte le operazioni di manutenzione che sono effettuate all'interno dell'Istituzione Scolastica avvengono con la supervisione del Responsabile del trattamento o dell'incaricato della manutenzione degli strumenti elettronici;
- **E' fatto assoluto divieto di memorizzare, sulla propria postazione di lavoro, dati di carattere personale che non siano inerenti alla funzione svolta;**
- E' proibito installare qualsiasi programma da parte dell'utente o di altri operatori, a meno che non siano autorizzati dell'Amministratore di Sistema o dal Responsabile del trattamento;
- E' vietato fare uso delle funzionalità di accesso remoto del proprio computer se non espressamente autorizzati dal Responsabile del trattamento o dell'amministratore di Sistema;
- Va evitato l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza;
- Va attivata la protezione massima per gli utenti del programmi di posta utilizzato, al fine di proteggersi dal codice html di certi messaggi e-mail, dato che alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer;
- **E' fatto divieto di utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi dello Stato;**
- Gli allegati di posta, di cui non sia certa la provenienza, non vanno aperti e in ogni caso vanno analizzati con un antivirus.

Elenco degli amministratori di sistema e relativi compiti.

Amministratore di sistema e relative mansioni:

Alex Moretto (Net at Work srl)

- Messa in opera delle richieste da parte della direzione dell'Istituto in materia di affidabilità e disponibilità dei sistemi, rispetto di politiche di sicurezza, privacy etc.).
- Progettazione ed implementazione di nuove soluzioni sia a livello infrastrutturale che applicativo.
- Installazione e configurazione di nuovo hardware e/o software lato server.
- Gestione account utente, account email, gruppi, politiche di accesso alla rete (in/out).
- Applicazione di patch/hotfix e di aggiornamenti necessari ai sottosistemi.
- Pianificazione della migliore politica di backup possibile con gli strumenti a disposizione, e proposte migliorative.
- Ottenimento delle migliori prestazioni possibili con l'hardware a disposizione (ottimizzazione delle risorse).
- Monitoraggio della struttura e degli apparati di rete.
- Implementazione e mantenimento di un sistema per la registrazione dei log di accesso amministrativi al sistema informativo.
- Aggiornamento dell'elenco degli ADS aggiunti e verifica attività secondo normativa.
- Documentazione delle operazioni effettuate.

Elenco amministratori di sistema aggiunti e relative mansioni:

Daniele Giuliani - Tecnico Sistemista

- Gestione account utente, account email, gruppi, diritti di accesso a cartelle di files ed applicazioni
- Gestione e verifica giornaliera dei backup
- Installazione, movimentazione, adeguamento e sostituzione PC e Thin Client (IMAC - Install Move Add & Change)
- Installazione e configurazione periferiche (Stampanti, Scanner etc..)
- Monitoraggio rete (verifiche connettività, rilevazione problemi e prestazioni
- Interventi di primo livello su malfunzionamenti sw e/o guasti hw

Stefano Pipia - Tecnico hardware, software

- Gestione account utente, account email, gruppi, diritti di accesso a cartelle di files ed applicazioni
- Gestione e verifica giornaliera dei backup

netatwork

- Installazione, movimentazione, adeguamento e sostituzione PC e Thin Client (IMAC – Install Move Add & Change)
- Installazione e configurazione periferiche (Stampanti, Scanner etc..)
- Monitoraggio rete (verifiche connettività, rilevazione problemi e prestazioni
- Interventi di primo livello su malfunzionamenti sw e/o guasti hw
- Gestione (Webmaster) dei contenuti del sito istituzionale liceodarwin.net

Paola Roccia – Collaboratore vicario del Dirigente

- Gestione degli account utente, password e diritti di accesso agli applicativi gestionali (registro elettronico).

Francesca Rolle – Collaboratore del Dirigente

- Gestione degli account utente, password e diritti di accesso agli applicativi gestionali (registro elettronico).

Data, 17 ottobre 2014

Amministratore di Sistema

Titolare trattamento dati