Direzione Sistemi Informativi

E-privacy e Intranet nella P.A.

Tutela della privacy e sicurezza aziendale

Direzione Sistemi Informativi

Servizio Sistemi in Rete ed Office Automation

Massimo Cappuccini

Firenze – 14 Giugno 2003
Salone de'Dugento
Palazzo Vecchio

e-Privacy 2003
Difesa dell'identità e della libertà d'espressione di fronte alla richiesta di sicurezza

Direzione Sistemi Informativi

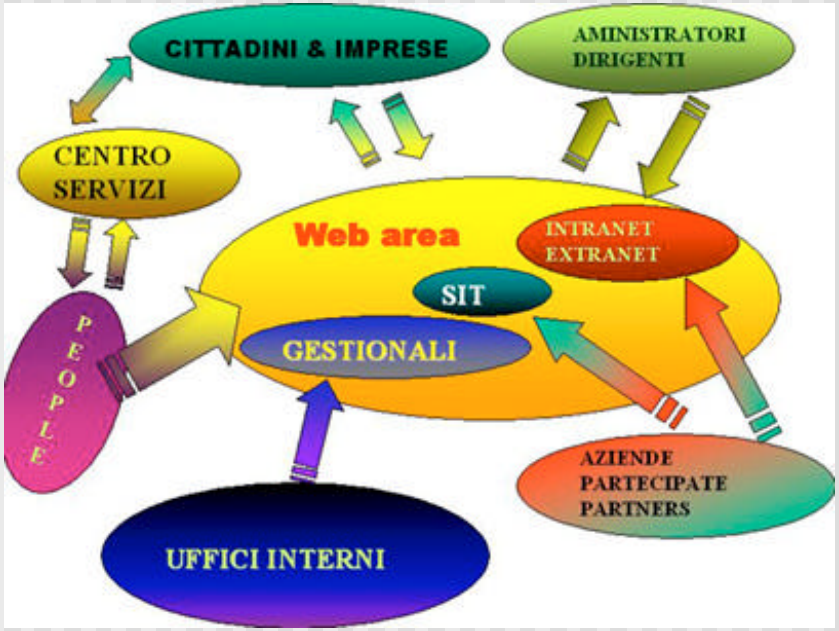
Mission della Direzione Sistemi Informativi

- Contribuire alla diffusione della cultura della sicurezza;
- Proporre metodi di analisi e soluzioni tecnico-organizzative per la realizzazione di sistemi che soddisfino i seguenti requisiti:
  - Integrità: Impedire modifiche dei dati da parte dei non autorizzati;
  - Continuità: Garantire il servizio informatico e la disponibilità dei dati a fronte di possibili interruzioni;
  - Disponibilità: Rendere accessibili i dati, entro prefissate finestre di erogazione del servizio, solamente a chi ne ha necessità per svolgere il proprio lavoro;
  - Riservatezza: I dati possono essere letti solo da coloro che sono autorizzati;
  - Verificabilità: Possibilità di ricostruire chi ha fatto cosa;
  - Governabilità: Capacità di rendere efficaci in tempi brevi le azioni normative, organizzative e tecniche finalizzate al miglioramento della sicurezza.

Direzione Sistemi Informativi

Contesto Tecnologico

- Sistemi Aziendali
  - 80 server
  - 2.800 Postazioni di lavoro
- Rete di connettività territoriale FI-Net
  - 35 nodi primari aziendali
  - 107 sedi secondarie
  - Aziende Partecipate e Enti Aderenti
- Applicazioni Aziendali e Banche Dati
- Servizi e connettività Internet
- Risorse
  - Strutture operative D.S.I.
  - Referenti Informatici
  - Consulenti e ditte specializzate di settore



Direzione Sistemi Informativi

Progettazione e mantenimento di un sistema informativo sicuro

- Definizione di livelli di servizio
- Azioni trasversali
- Azioni sui sistemi server
- Azioni sulle postazioni di lavoro
- Azioni sulle applicazioni e banche dati
- Azioni organizzative

Direzione Sistemi Informativi

Livelli di servizio

Disponibilità controllata delle informazioni

Il sistema deve rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.

Fattori critici:

•Robustezza del sw di base ed applicativo;

•Affidabilità delle apparecchiature e degli ambienti

•Esperienza ed affidabilità degli amministratori di sistema

Al fine di garantire la continuità del servizio, fra gli obiettivi di una politica di sicurezza deve esserci anche la gestione del disaster recovery.

Integrità delle informazioni

Il sistema deve impedire l'alterazione diretta o indiretta delle informazioni (compresa la perdita di dati), voluta o accidentale.

Riservatezza delle informazioni

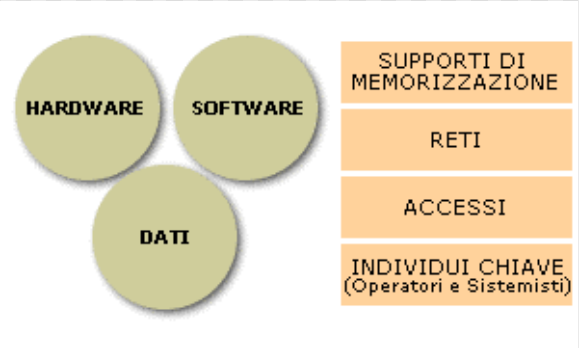
In determinati contesti, il fatto stesso che una informazione sia protetta, o che esista una comunicazione in atto fra due utenti o processi, può essere sufficiente per dedurre informazioni riservate.

Supporto agli utenti

Direzione Sistemi Informativi

Azioni Trasversali

- Sistema dei domini
- Controllo accessi fisici e logici
- Antivirus centralizzato
- Hardering dei sistemi



- Firma digitale qualificata
- Certificati di sicurezza
- Archiviazione ottica e conservazione
- Sistemi di backup-centralizzati
- Gestione dei supporti

- Configurazione sicura dei Router
- Architettura Proxy / Firewall
- VPN
- Fault-Tolerance Rete
- Disaster-Recovery

- Work-Flow dei Processi
- Acceptable User Policy
- Formazione
  - *Personale tecnico specialistico*
  - *Referenti informatici*
  - *Utenti finali*

Direzione Sistemi Informativi

Azioni sui sistemi server

- Sistemi ridondati
- Clustering
- Installazione dei servizi essenziali
- Livelli di protezione differenziati, sulla basa dell'analisi del rischio
- Aggiornamento patch sistemi operativi ed applicazione dei bollettini di sicurezza
- Monitoraggio delle prestazioni
- Log Analysis
- Ethical Hacking

Direzione Sistemi Informativi

Azioni sulle postazioni di lavoro

- Password BIOS
- Password Screen-Saver
- Livelli di protezione differenziati, sulla basa dell'analisi del rischio
- Aggiornamento patch sistemi operativi ed applicazione dei bollettini di sicurezza
- Help Desk e Gestione Interventi

Direzione Sistemi Informativi

Azioni sulle applicazioni e le banche dati

- Promozione dello sviluppo di applicazione Web-Based via HTTPS
- Convergenza dei Data Base
- Crittografia
- Definizione dei modelli di esposizione dei dati su Legacy e dei metodi / autorizzazioni di accesso

Direzione Sistemi Informativi

Azioni organizzative

- Gruppo direttivo sicurezza (regolamenti, direttive)
- Il documento di policy
  - Direttive per la sicurezza dei servizi di rete
  - Definizione dei livelli di servizio dell'Ente
  - Regolamento di accesso ai servizi di rete
  - Norme di attuazione del regolamento di Policy anche nei confronti di soggetti esterni
- Regolamento per il trattamento di dati personali
- Definizione di strutture, ruoli e responsabilità

Direzione Sistemi Informativi

Nella pratica ...(1/7)

Circolazione dei dati personali sensibili cartacei

I dati sensibili devono essere tutelati anche nella fase di circolazione affinché siano distribuiti solo alle persone autorizzate

- I dati sensibili devono poter essere consegnati direttamente alla persona interessata. In alternativa, servendosi di posta interna o fornitore esterno, si utilizzano buste sigillate da consegnarsi solo alle persone autorizzate al ritiro .
- Le comunicazioni ritenute urgenti sono eseguite tramite avviso telefonico alla persona autorizzata.
- I dati sensibili sono stampati solo in presenza di una persona autorizzata
- Le stampanti remote e le apparecchiature ausiliarie devono, quando possibile, essere ubicate in locali ad accesso controllato .

Controllo Accessi ai Sistemi

I dati personali e sensibili devono essere resi disponibili unicamente alle persone autorizzate e che ne hanno necessità per lo svolgimento dei compiti loro assegnati.

Il Responsabile del Trattamento di dati sensibili verifica e autorizza le richieste di accesso ai sistemi contenenti dati sensibili sulla base delle specifiche necessità di accedere ai dati e di trattarli. L'autorizzazione è accompagnata da nomina formale a incaricato del trattamento

Il Responsabile del Trattamento di dati sensibili segnala, tempestivamente, al Responsabile della Sicurezza Informatica ogni modifica organizzativa che abbia un qualsiasi effetto sulle autorizzazioni rilasciate

L'Amministratore di Sistema predispone a sistema il profilo di accesso autorizzato, generando la password e l'utenza e le comunica all'utente

L'utenza è personale e di uso esclusivo dell'utente cui è assegnata.

La riservatezza della password è responsabilità dell'utente che ne è proprietario.

Direzione Sistemi Informativi

Nella pratica ...(2/7)

Procedure di salvataggio dati e loro custodia: uffici (PC e stazioni di lavoro)

I dati sensibili non devono essere memorizzati su PC: ogni eccezione deve essere controllata e gestita. I dati aziendali devono essere salvati su sistemi centrali e/o file server, evitando di memorizzarli localmente sulla propria stazione di lavoro.

Il trasferimento di dati personali, sensibili all'esterno deve essere autorizzato e giustificato dal Responsabile del Trattamento dei dati sensibili.

Eventuali dati personali sensibili che temporaneamente non possono essere salvati su sistemi centrali o file/server devono essere salvati su floppy conservati in armadi chiusi a chiave. I floppy devono essere formattati o distrutti non appena sarà possibile scaricare i dati sui sistemi centrali o file/server.

Ogni copia di dati personali/sensibili, è custodita in armadi chiusi a chiave: l'eventuale diffusione delle copie di dati personali sensibili deve essere preventivamente autorizzata dal Responsabile del Trattamento dei dati sensibili.

Gestione di nuove Banche Dati Sensibili

Il trattamento di una nuova Banca Dati "Sensibili" deve essere autorizzata, notificata e gestita tramite il Documento Programmatico sulla Sicurezza dei Dati.

I Responsabili del Trattamento nominati devono concordare con il Titolare ogni esigenza di nuovi trattamenti di dati sensibili non inclusi nel presente documento.

Se il trattamento in oggetto è approvato, il Responsabile del Trattamento coinvolto provvede, prima dell'inizio del trattamento, ad informare il Responsabile di Privacy e Sicurezza affinché richieda autorizzazione al trattamento e quindi effettui notificazione integrativa.

Il Responsabile del Trattamento coinvolto, avvalendosi di volta in volta delle figure necessarie all'implementazione delle misure di sicurezza (rif. procedure aziendali di sicurezza) provvede all'analisi e implementazione delle misure stesse ed all'aggiornamento del Documento Programmatico sulla Sicurezza dei dati.

Direzione Sistemi Informativi

Nella pratica ...(3/7)

Le attività al computer

Non rimuovere o aggiungere alcuna apparecchiatura o componente della stazione di lavoro, salvo specifica autorizzazione .

Spegnere il terminale a fine lavoro

Attivare la schermata di protezione del PC quando ci si allontana dalla propria postazione di lavoro per la pausa pasto, una riunione o altro

Non copiare dati personali sulla propria stazione di lavoro o sui serventi locali (LAN), se non previamente autorizzato

Lo scarico di dati su dischetto deve essere giustificato, autorizzato e documentato, in particolare se trattasi di dati personali

Non estrarre, trasmettere, divulgare tramite supporti informatici dati personali che sono trattati per svolgere la propria mansione

E' vietato distruggere, deteriorare, sottrarre, duplicare, riprodurre o rendere del tutto od in parte inservibili i sistemi informatici od i programmi, le informazioni o i dati presenti nel sistema aziendale

Le attività in ufficio

E' necessario proteggersi da accessi non autorizzati ricordandosi di:

Chiudere le porte

Chiudere le finestre

Chiudere i cassetti

Riordinare a fine giornata, o nelle pause prolungate, le varie cartelle, schede e dischetti

Custodire le chiavi

Non lasciare documenti con dati riservati e importanti (es. informazioni sui clienti o sul personale) nella fotocopiatrice o sulla scrivania

Direzione Sistemi Informativi

Nella pratica ...(4/7)

Comunicazioni telefoniche

Effettuare le comunicazioni relative a dati personali e/o sensibili in un luogo riservato o chiuso .

Non comunicare né lasciare nella memoria della segreteria telefonica messaggi relativi a dati sensibili

Dotare la casella vocale, o segreteria telefonica, di codice personale per accesso all'ascolto (se possibile)

Gestione della Posta verso l'esterno

Per quanto riguarda la comunicazione di dati personali tramite il servizio di Posta:

- Dati personali: deve essere limitata / controllata e custodita
- Dati sensibili: deve essere limitata e preferibilmente vietata

Archivi cartacei e schedari

Custodirli in aree protette e controllate

Fare attenzione alla loro chiusura (aprirli solo quando necessario)

Fare costante attenzione alle scadenze dei termini di conservazione dei documenti per procedere alla loro distruzione

Custodire le proprie chiavi

Stampe

Indirizzare verso una stampante dedicata, collocata in un'area limitata e controllata, le stampe di dati personali / sensibili

Non dimenticare documenti riservati sulla stampante

Direzione Sistemi Informativi

Nella pratica ...(5/7)

Riproduzione dati

Dati personali: deve essere limitata e controllata a fronte di una lista di distribuzione

Dati sensibili: deve essere autorizzata dal Responsabile del trattamento

Distruzione dati

Distruggere i dati sensibili/personali tramite il "trituratore", evitare di cestinarli .

Utilizzare un regolare servizio di macero, impedendo agli addetti la visibilità dei documenti

Trasmissione dati via fax

Non utilizzare il Fax per la trasmissione di dati sensibili; se fosse necessario comunicare l'invio e richiedere il presidio, lo stesso vale per il ricevimento

Dare avviso della trasmissione di dati personali al ricevente

Presentazioni

Utilizzare dati privi di qualsiasi riferimento o codice di collegamento a persone fisiche o giuridiche per le presentazioni

In viaggio

Garantire adeguata custodia dei documenti dei supporti informatici che contengono dati personali e/o sensibili

Non consultarli in luogo pubblico

Direzione Sistemi Informativi

Nella pratica ...(6/7)

Accesso alle risorse informatiche: utenze e password

Ogni utente autorizzato può accedere, tramite risorse informatiche, a dati personali facendosi riconoscere digitando sul PC il proprio codice utente e la propria password.

Entrambi devono essere gestiti secondo le seguenti istruzioni.

In ogni caso è vietato introdursi nel sistema informatico in maniera abusiva o declinando false generalità.

Codice utenza (user-id)

L'utente deve farne un uso strettamente personale (ovvero non la deve condividere con altri), operando esclusivamente nell'ambito delle autorizzazioni ricevute e utilizzando le risorse solo per svolgere il proprio lavoro o comunque per scopi aziendali.

L'utenza è quindi:

- personale ed univoca nel tempo
- revocata quando l'utente non ha più necessità di accedere al sistema
- rivista annualmente dal responsabile del trattamento (verifica di conformità)

Password

È una parola definita e nota solo all'utente; è strettamente personale e non deve essere resa nota ad altri per nessun motivo. Le regole per la scelta e la protezione delle password sono:

La password è scelta a caso, non è ovvia, banale o di facile individuazione

Deve essere cambiata al primo utilizzo dopo il suo rilascio o qualora sorgessero dubbi circa la sua conoscenza da parte di altri utenti

Non deve essere visibile sul terminale quando digitata (né deve essere scritta su fogli "volanti" o appesi al video, al calendario o alla lavagna dell'ufficio)

Direzione Sistemi Informativi

Nella pratica ...(7/7)

Accessi ad Internet

I collaboratori autorizzati ad accedere ad Internet devono utilizzare solo i servizi cui sono abilitati

La navigazione deve essere effettuata in modo etico e solo al fine di migliorare la propria produttività.

Gli accessi ad Internet attraverso la rete aziendale sono controllati e registrati attraverso strumenti di firewall

Quando richiesto, devono essere declinate le proprie generalità.

I collaboratori sono tenuti al rispetto della regolamentazione del copyright anche per i programmi freeware e shareware scaricati dalla rete.

I programmi disponibili possono contenere virus: osservare gli standard previsti in materia.

Non devono essere messi a disposizione materiali a carattere inappropriato od offensivo, ed è comunque vietato accedervi.

Non devono essere messe a disposizione di terzi informazioni a carattere riservato o personale.

Posta elettronica

È uno strumento a disposizione per attività aziendali e non è consentito l'uso per fini personali

Le misure di sicurezza per la trasmissione dei messaggi deve essere coerente col valore delle informazioni trattate. Le informazioni riservate o relative a dati personali/ sensibili devono essere trasmesse solo se opportunamente protette (crittografia).

Non sono permesse le catene di S. Antonio nè è tollerato lo scambio di messaggi in conflitto con l'etica professionale o con gli interessi dell'azienda

Antivirus

Su tutte le stazioni di lavoro è presente un prodotto antivirus mantenuto aggiornato automaticamente; nel caso in cui il sistema rilevi la presenza di un virus sulla stazione di lavoro contattare immediatamente l'Help Desk

Link

http://www.sans.org/infosecFAQ/policy/policy_list.htm

http://www.ietf.org/rfc/rfc2196.txt?Number=2196

http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf

http://www.security.kirion.net/securitypolicy/

http://www.network-and-it-security-policies.com/

http://www.brown.edu/Research/Unix_Admin/cuisp/

http://iatservices.missouri.edu/security/

http://www.utoronto.ca/security/policies.html

http://irm.cit.nih.gov/security/sec_policy.html

http://w3.arizona.edu/~security/pandp.htm

http://secinf.net/ipolicye.html

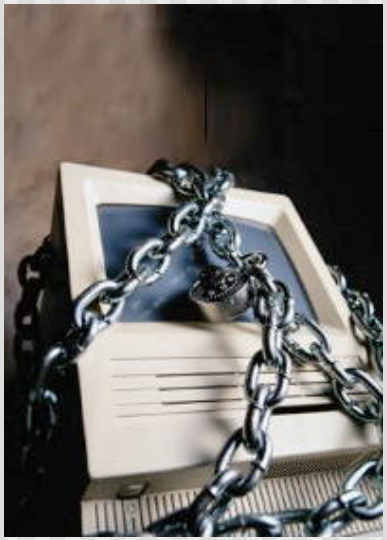
http://ist-socrates.berkeley.edu:2002/pols.html

http://www.ruskwig.com/security_policies.htm

http://razor.bindview.com/publish/presentations/InfoCarePart2.html

http://www.jisc.ac.uk/pub01/security_policy.html

Direzione Sistemi Informativi



DOMANDE E RISPOSTE

Firenze – 14 Giugno 2003
Salone de'Dugento
Palazzo Vecchio

e-Privacy 2003 - Difesa dell'identità e della libertà d'espressione di fronte alla richiesta di sicurezza