PRIVACY

Linee Guida per la corretta applicazione del testo unico sulla sicurezza e la privacy delle Informazioni

IL TESTO UNICO : Dlgs 30 Giugno 2003 n. 196

Il Dlgs 30 giugno 2003, n. 196, pubblicato in Gazzetta Ufficiale il 29 luglio 2003, ha introdotto il testo unico delle disposizioni in materia di:

tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

Il testo unico assume le caratteristiche di un vero e proprio :

Codice Privacy

In un unico testo vengono raccolte, coordinate ed armonizzate tutte le precedenti disposizioni contenute in una miriade di provvedimenti, che vengono di conseguenza abrogati.

IL CODICE

“Chiunque ha diritto alla protezione dei dati personali che lo riguardano” (art.1)

“Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali” (art.2)

PRINCIPI GENERALI

Il PRINCIPIO DI NON ECCEDENZA

Impedire che grazie alle nuove tecnologie vengano costruiti enormi database nei quali siano racchiuse quante più informazioni possibili sugli individui: dalla religione alla marca di tonno acquistata al supermercato

DISPOSIZIONE ANTISCHEDATURA

I principi di fondo della privacy, pur essendo stati celati, nei primi anni di applicazione della nostra legislazione burocratica e burocratizzante, da una montagna di carte, altro non sono che la traduzione in legge della

BUONA EDUCAZIONE

Le informazioni personali sono un qualcosa che appartiene ad altre persone, che va maneggiato con cura e discrezione per non violare la dignità e la riservatezza degli individui interessati.

I DATI PERSONALI

IL DATO PERSONALE E' UNA INFORMAZIONE SU UN SOGGETTO

Qualunque informazione (compresi suoni e immagini) relativa ad una persona fisica, giuridica, ente od associazione identificati o identificabili anche indirettamente mediante riferimento o qualsiasi altra informazione ivi compreso un numero di identificazione personale

La legge ha individuato le seguenti categorie di dati personali:

- **DATI COMUNI**
- **DATI SENSIBILI**
- **DATI GIUDIZIARI**
- **DATI DI NATURA COMUNE, MA IL CUI TRATTAMENTO PRESENTA RISCHI SPECIFICI**

I DATI SENSIBILI E GIUDIZIARI Art. 4 lettere d) ed e)

Toccano la sfera più intima del soggetto e possono essere utilizzati con intenti discriminatori o persecutori.

*"**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*

*"**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*

SU QUESTI DATI E' NECESSARIO GARANTIRE LA MASSIMA TUTELA

DATI PARTICOLARI

il cui trattamento presenta rischi specifici

ESEMPIO :

MARIO ROSSI E' NATO A TERAMO IL 2 MARZO DEL 1950

DATO COMUNE

ABRAMO LEVI E' NATO A TEL AVIV IL 2 MARZO DEL 1950

DATO PARTICOLARE

In questo caso la semplice combinazione di elementi anagrafici "di base" può svelare una precisa informazione in merito alla **religione** ed al **gruppo etnico** di appartenenza del soggetto

TRATTAMENTO DEI DATI

Qualsiasi operazione che concerne la raccolta, modifica, cancellazione, registrazione, conservazione, raffronto, utilizzo, diffusione, comunicazione, ecc. dei dati:

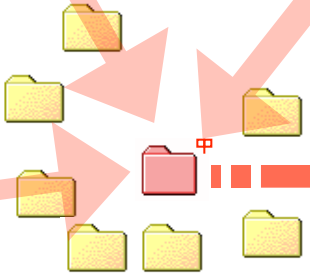
IN PRATICA TUTTO CIÒ CHE PUÒ ESSERE FATTO CON I DATI

ESEMPIO DI SCHEDATURA

Cellulare

Autostrade

Acquisti



ARCHIVIO

GLOBALE

PERCHE' PROTEGGERE LE INFORMAZIONI?

- Utilizzo non autorizzato di informazioni personali
- Furto d'identità (ID Theft – FBI's #1 crime)
- Perdita di reputazione anche se ingiustamente accusato
- Ricevere un trattamento da criminali per operazioni illecite commesse dai vostri sistemi.

FALSE IDENTITA’

IDENTACARD

Welcome to iDentacard

www.identacard.co.uk

Home of the world's most effective fake ID's!

- HOME
- CARDS
- ORDER
- FAQ
- CONTACT US
- LINKS

THE ULTIMATE IDENTACARD IN FAKE ID

All of our cards are Credit Card size and thermally printed onto PVC
ONLY THE MOST EFFECTIVE!

European Identity 4
Another unbeatable fake ID from iDentacard, The European Identity Card 4.

The front has your Name, Nationality, and Date of Birth together with your photo and signature and an **embossed** issue code.

The photo is overlaid with a European flag security mark, and the signature and your details are covered by atlas and wavy line details!

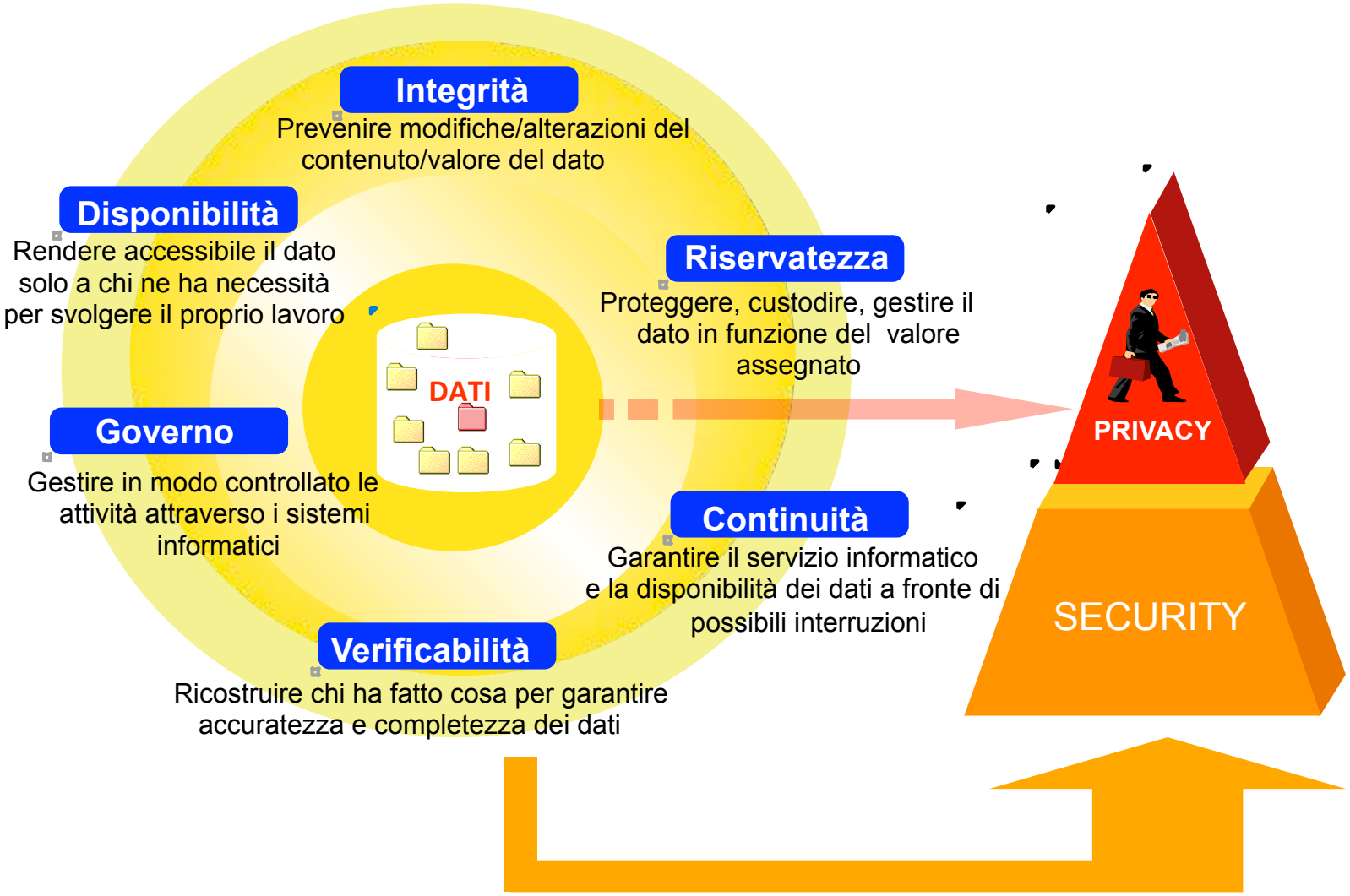
The back of the card holds a magnetic strip together with general card information.

These are low quality scans so as to make them load faster! Remember the actual cards are photo quality and we offer a full refund if you're not satisfied!

PRICE: £10.00

Click here to order!

PROTEZIONE DEI DATI PERSONALI



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

1. **Redatto entro il 31 marzo di ogni anno**
2. **Deve contenere:**
   - **l'elenco dei trattamenti di dati personali**
   - **la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento**
   - **l'analisi dei rischi che incombono sui dati**
   - **le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;**
   - **la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento**
   - **la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati**
   - **la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare per i dati personali idonei a rivelare lo stato di salute e la vita sessuale l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato**
3. **Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza**

TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Trattamento **consentito solo se** sono adottate le seguenti misure minime (art.34) :

A. autenticazione informatica;
B. adozione di procedure di gestione delle credenziali di autenticazione;
C. utilizzazione di un sistema di autorizzazione
D. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti ed a determinati programmi informatici;
E. adozione di procedure per l'adozione di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
F. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito agli incaricati ed agli addetti alla gestione o alla manutenzione degli strumenti elettronici;
G. Tenuta del Documento Programmatico sulla Sicurezza;
H. Tecniche di cifratura per trattamenti di dati idonei effettuati da organismi sanitari.

AUTENTICAZIONE INFORMATICA

Gli incaricati devono essere dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o ad un insieme di trattamenti.

Credenziali di autenticazione :

- **Codice per l'identificazione** dell'incaricato associato ad una **parola chiave riservata** conosciuta solamente dal medesimo
- **Dispositivo di autenticazione** in possesso ed uso esclusivo (badge, smart card), anche associato a codice identificativo o parola chiave
- **Caratteristica biometrica** dell'interessato (iride, impronta digitale), anche associato a codice identificativo o parola chiave


APPLICAZIONE
SISTEMA DI AUTENTICAZIONE
USERNAME
PASSWORD
Connect to w2kfs0.csrv.ad.york.ac.uk
Connecting to userfs
User name:
ozw1@york.ac.uk
Password:
OK
Cancel
DISPOSITIVO
AUTENTICANZIONE
BIOMETRIA
UTENTE

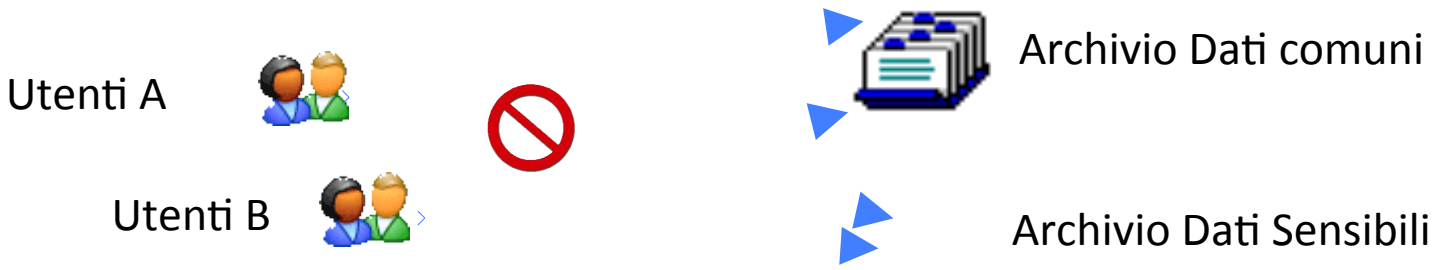
CODICE E PAROLA CHIAVE

1. Ogni codice (ad es. username) può essere utilizzato da **un solo incaricato** e non può essere assegnato ad altri incaricati, neppure in tempi diversi
2. Ad ogni incaricato possono eventualmente essere assegnati **più codici** per l'identificazione (ad esempio per funzioni diverse)
3. La Parola Chiave (ad es. Password) è Riservata e conosciuta **solamente** dall'incaricato
4. L'incaricato deve assicurare la riservatezza della parola chiave
5. La lunghezza minima della parola chiave è di **otto caratteri** (nei sistemi che lo permettono)
6. La parola chiave non contiene riferimenti agevolmente riconducibili all'incaricato
7. La parola chiave viene modificata al primo utilizzo
8. Modificata ogni **sei mesi** oppure ogni **tre mesi** (trattamento di dati sensibili o giudiziari)
9. Le credenziali di autenticazione non utilizzate da **almeno 6 mesi** devono essere **disattivate** (tranne quelle usate per soli scopi di gestione tecnica)
10. Le credenziali devono essere **disattivate** in caso di **perdita della qualità** che consente l'accesso ai dati

SISTEMA DI AUTORIZZAZIONE

- **Sistema di autorizzazione**: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati ed alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

- **Profilo di autorizzazione**: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.



PROTEZIONE DEI SISTEMI INFORMATIVI

Tutti i sistemi di elaborazione (server, client) devono essere protetti dal rischio costituito da **virus informatici** e simili

La protezione deve essere attiva anche per i sistemi non connessi in rete o che non accedono a internet

Gli utenti **non devono** poter disattivare l'antivirus

L'aggiornamento deve essere obbligatoriamente almeno semestrale, **ma è necessario – per la sicurezza del sistema informatico aziendale – che sia quotidiano o al massimo settimanale!**

PROTEZIONE DEI SISTEMI INFORMATIVI

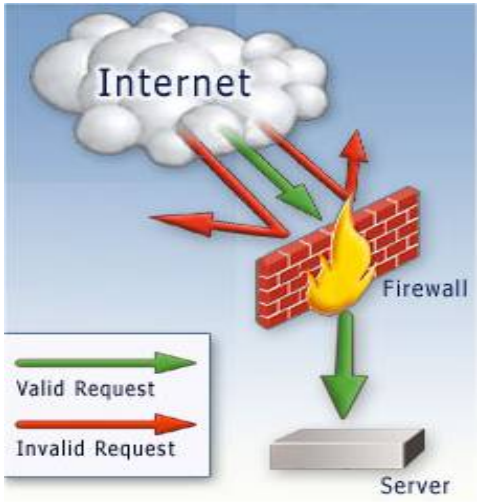
Aggiornamenti di programmi per elaboratore volti a:

- **Prevenire la vulnerabilità di strumenti elettronici**
- **Correggere difetti**

- Devono essere eseguiti con cadenza almeno **annuale**
- In caso di trattamento di dati sensibili o giudiziari con cadenza **almeno semestrale**

PROTEZIONE DEI SISTEMI INFORMATIVI

Sistema anti-intrusione informatica



- **Firewall**

Un apparato che separa regolamenta e protegge la rete aziendale dalle reti esterne (ad es. Internet)

- **I**ntrusion **D**etetection **P**revention

Un apparato che analizza il traffico di rete e previene attività anomale che potrebbero causare situazioni critiche.

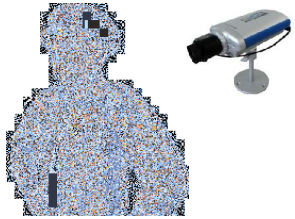
PROTEZIONE DEI SISTEMI INFORMATIVI

Protezione delle aree e dei locali

(generali o specifici ai locali informatici)

- Sistemi anti-intrusione

- Vigilanza e controllo accessi



- Sistemi anti-incendio

SALVATAGGIO E MODALITA' PER IL RIPRISTINO DEI DATI

E' **obbligatorio** il salvataggio dei dati personali (backup) La frequenza di salvataggio deve essere almeno **settimanale**, ma è opportuno che sia **quotidiana**

Devono essere protetti **tutti** i dati:

Sistemi gestionali o ERP
Documenti degli utenti
Posta elettronica
…

Devono essere impartite **istruzioni (scritte)** di carattere tecnico ed organizzativo per definirne le modalità di esecuzione

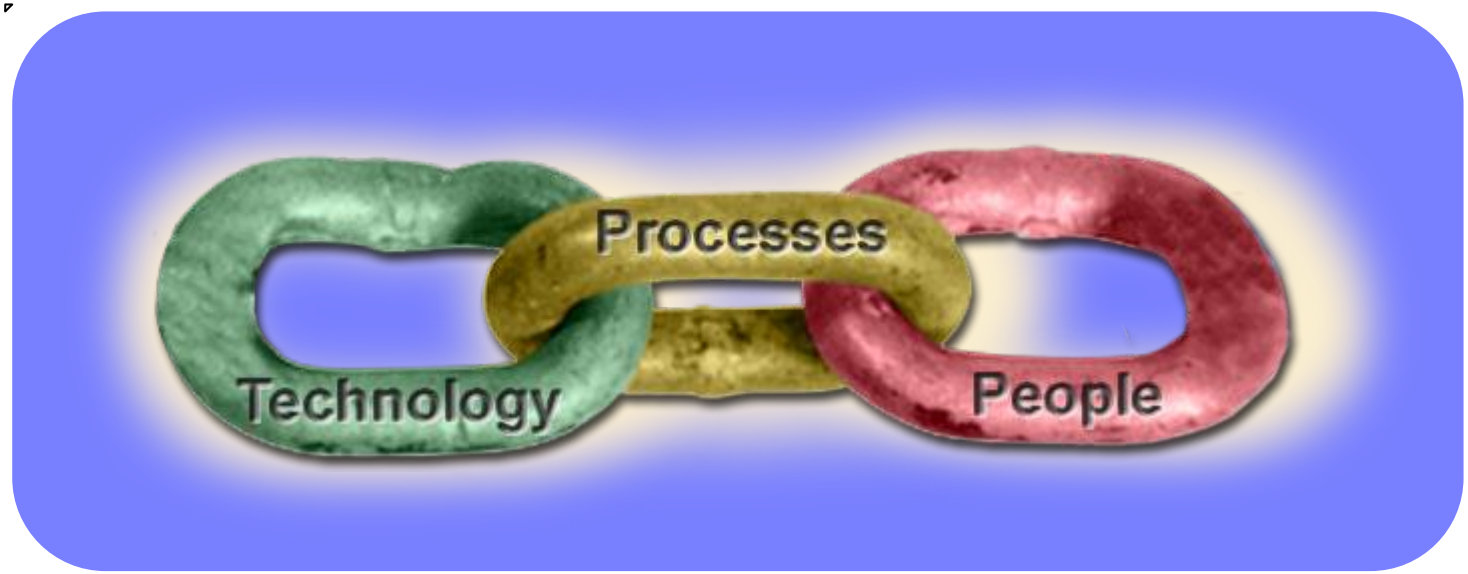
- Ai Sistemi Informativi si deve assicurare la continuità di alimentazione

- Si consigliano Sistemi ridondanti o ad alta affidabilità (RAID, Cluster,etc)

- Disaster recovery : deve essere garantito l'accesso ai dati in caso di incidente (danneggiamento dei dati o degli strumenti) in **tempi certi** e comunque non superiori a **sette giorni**

LA TECNOLOGIA E' SOLO UN ASPETTO

I sistemi sicuri dipendono da Tecnologia, Processi e Persone



UN SISTEMA È TANTO "DEBOLE"
QUANTO L'ANELLO PIÙ DEBOLE DELLA SUA CATENA

ESEMPIO

Il fattore umano: l'anello più debole ?

La convincente disciplina del "social engineering"

Un esempio classico a livello di azienda è la persona che spacciandosi per un tecnico informatico telefona ad un impiegato, e dopo aver descritto una situazione di pericolo sul suo computer, propone una soluzione urgente in cui l'impiegato deve fornire una serie di informazioni che possono arrivare fino alla password. A questo punto, indipendentemente da quanto l'azienda abbia investito nella sua infrastruttura di sicurezza, con questo semplice stratagemma l'hacker può ottenere tutte le informazioni desiderate e il gioco è fatto!

Attacchi ti questo tipo, caratteristici dell'ambito aziendale, sono ormai molto diffusi con modalità leggermente differenti anche nell'ambito domestico (**Phishing**)

REGOLAMENTO E FORMAZIONE

Interventi formativi

Riguardano:

- Conoscenza dei rischi
- Conoscenza delle misure di sicurezza e dei comportamenti da adottare
- Responsabilità

Devono essere erogati:

- Al momento dell'ingresso in servizio
- In occasione di cambio di mansioni
- In occasione dell' introduzione di nuovi strumenti
- E' opportuno che siano documentati

PER SAPERNE DI PIU’

www.garanteprivacy.it