

SICUREZZA DELLE INFORMAZIONI
Nuovi scenari e strategie di sicurezza

MASSIMO CHIUSI

Responsabile Sicurezza delle Informazioni - Unicredito Italiano

LO SCENARIO DI RIFERIMENTO

Lo scenario di riferimento
L'evoluzione tecnologica richiede una "sicurezza trasversale"
Ed un'integrazione tra la sicurezza fisica e logica

Approccio Tradizionale

Tangible Asset
Protection



➔

Computer Crime

Untangible Asset
Protection



CRISI DELLA PRECEDENTE STRUTTURA ORGANIZZATIVA

Sono necessarie nuove strategie di sicurezza !



E' ora necessario proteggere anche i dati, le informazioni e la "moneta elettronica"...

Documento riservato - riproduzione anche parziale vietata

3

Unicredito Italiano

Lo scenario di riferimento
La sicurezza delle informazioni è un problema che è correlato a processi, tecnologie e persone

I Processi di sicurezza delle informazioni

Le tecnologie utilizzate

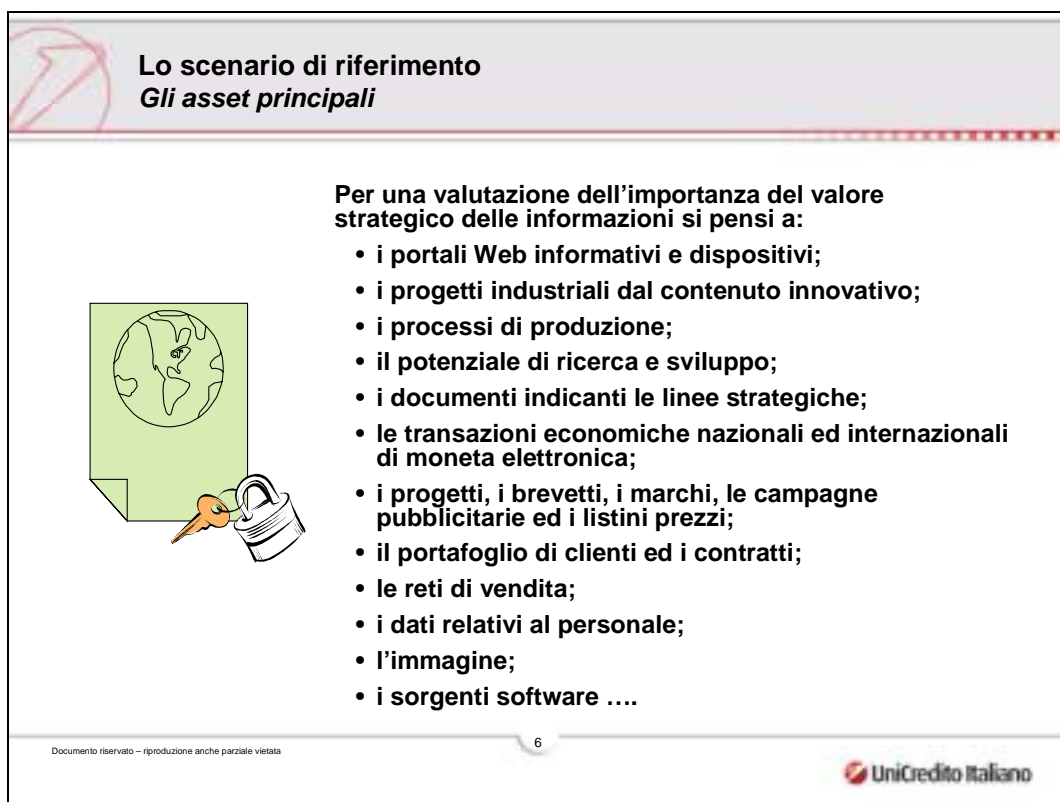
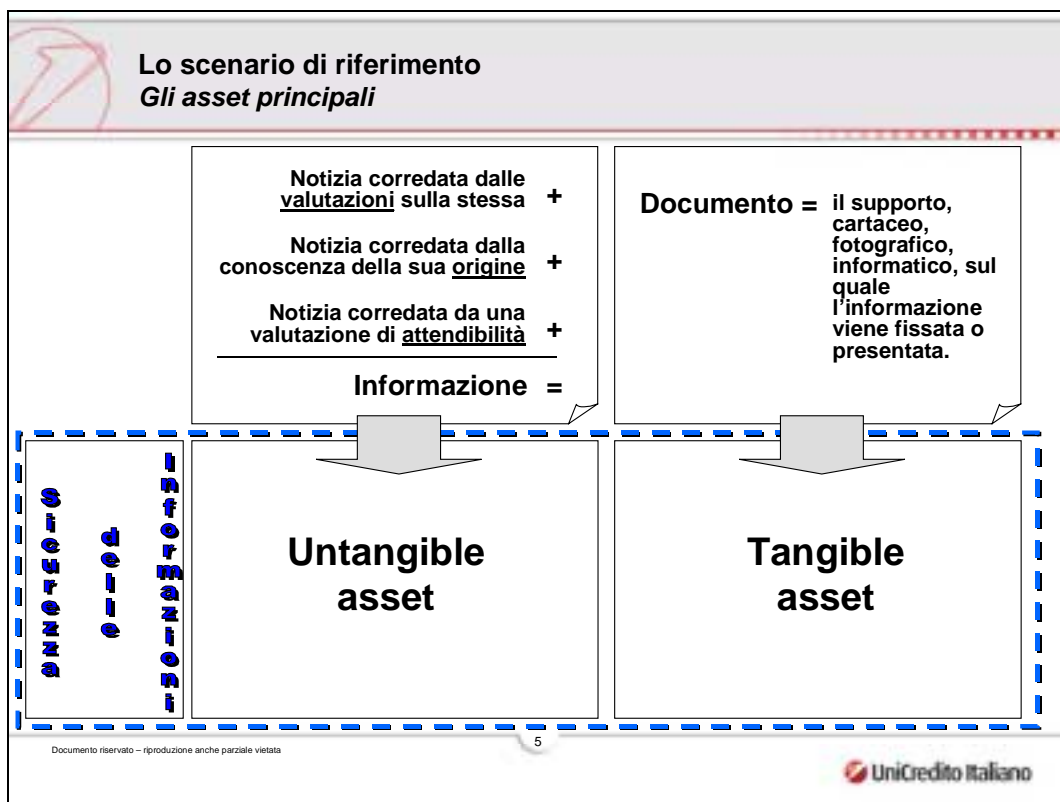
La formazione del Personale

- Analisi dei fenomeni e dei rischi
 - Gestione "Osservatori On-line"
 - Data base degli eventi rilevati
 - Studi di contromisure difensive
- Architetture PKI e smart card
 - Standard certificati e collaudati
 - Policies di Gruppo
 - Strumenti e prodotti specifici
- Incarichi specifici al Personale
 - Formazione di Privacy e Sicurezza
 - Sicurezza come priorità aziendale
 - Coinvolgimento di tutti i ruoli

Documento riservato - riproduzione anche parziale vietata

4

Unicredito Italiano



I DRIVER DI CAMBIAMENTO



I Driver:
Trasformare la sicurezza da costo a investimento

Sicurezza: da costo a necessità

La Legge 23 Dicembre 1993 n. **547 (Criminalità Informatica)**, la Legge 31 dicembre 1996 n. **675 (Trattamento dei Dati Personali)**, il D.Lgs. n. **231/2001** e recentemente il **D.Lgs. 196/03 "Codice in materia di protezione dei dati personali"** hanno cambiato lo scenario:

➔


La Sicurezza delle Informazioni non deve essere più considerata solo un **COSTO** ma una **NECESSITA'** per l'Amministratore per evitare rischi ed anche un vantaggio competitivo ...



Documento riservato - riproduzione anche parziale vietata

8





I Driver:
La Legge n. 675/1996 sulla privacy ed il d.P.R. n. 318/1999

L'obbligo di legge ha rappresentato un'occasione per introdurre in azienda una normativa complessiva sulla trattazione delle informazioni inclusa la loro classificazione e l'analisi dei rischi

La redazione del Documento Programmatico sulla Sicurezza ha finora principalmente individuato:

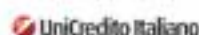
- I rischi riferiti ai trattamenti
- I criteri tecnici ed organizzativi per la protezione di aree e locali e per controllare l'accesso delle persone
- I criteri e le procedure per assicurare l'integrità dei dati
- I criteri e le procedure per la sicurezza della trasmissione dei dati
- L'elaborazione di un piano di formazione edotti gli incaricati circa il trattamento dei rischi

Al di là della tutela giuridica, le contromisure ad oggi attuate al fine di proteggere le informazioni sono:


- Evitare la continua e superflua trasmissione di informazioni
- Individuare con precisione le informazioni da proteggere con relativa classificazione
- Proteggere queste informazioni con adeguate misure di sicurezza fisiche, procedurali, organizzative e logiche adeguatamente integrate tra loro

Documento riservato - riproduzione anche parziale vietata

9



I Driver:
La Legge n. 675/1996 sulla privacy ed il d.P.R. n. 318/1999


<p>Il d.P.R. 318/1999, redatto in applicazione dell'articolo 15 della legge 675/96 ha regolamentato le norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali</p>	 <p>Riservatezza e Diritto di informazione</p>
 <p>Pretesa della custodia sicura</p>	

Documento riservato – riproduzione anche parziale vietata

10



I Driver:
La Legge n. 675/1996 sulla privacy ed il d.P.R. n. 318/1999




Il d.P.R. 318/99, in applicazione dell'art. 15 della 675/96, ha regolamentato l'individuazione delle misure minime di sicurezza per garantire la protezione dei dati.
Per valutare l'idoneità di tali misure, si fa riferimento alle conoscenze tecniche del momento, alla natura dei dati, alle caratteristiche del trattamento ed ai rischi.

La sicurezza assume quindi una concezione dinamica che comprende misure di sicurezza organizzative, gestionali, fisiche e logiche che devono tenere conto dell'evoluzione tecnica intervenuta e dell'esperienza maturata nell'ambito del comparto della sicurezza.

Documento riservato – riproduzione anche parziale vietata

11



I Driver:
Il Decreto 231/2001 sulla responsabilità amministrativa delle Società

Responsabilità	Reati	Soggetti
<p>Il decreto in oggetto introduce e disciplina una responsabilità degli Enti a titolo di illecito conseguente a reato commesso da persone fisiche riconducibili allo stesso Ente e si applica sia agli Enti dotati di personalità giuridica sia alle società ed associazioni che ne sono prive.</p>	<p>Lo stesso identifica quali sanzionabili i reati di:</p> <ul style="list-style-type: none"> • indebita percezione di erogazioni; • truffa in danno dello Stato o di un Ente pubblico o per il conseguimento di erogazioni pubbliche; • frode informatica in danno dello Stato o di un Ente pubblico; • concussione; • corruzione. 	<p>I soggetti che avendo commesso il reato determinano la conseguente responsabilità penale ed amministrativa dell'Ente possono essere sia coloro che si trovino in una <u>posizione apicale</u>, sia coloro che sono sottoposti alla direzione o vigilanza dei primi.</p>

Documento riservato - riproduzione anche parziale vietata

12



I Driver:
Il Decreto 231/2001 sulla responsabilità amministrativa delle Società



La frode informatica è specificamente regolata dall'art. 640-ter del *Codice Penale* e si riferisce alla necessità di impedire o reprimere l'ipotesi di illecito arricchimento attraverso una interferenza con il regolare svolgimento di un processo di elaborazione dati al fine di ottenere uno spostamento patrimoniale ingiustificato.

Il sistema di controllo dovrebbe prevedere, tra l'altro l'adozione di:

- un Codice Etico;
- un *sistema organizzativo che formalizzi i processi*;
- *procedure manuali ed informatiche* che prevedano punti di verifica;
- poteri autorizzativi e di firma distinti;
- *sistemi di segnalazione dell'esistenza di situazioni critiche*;
- comunicazioni al personale e relativa formazione.


Documento riservato - riproduzione anche parziale vietata

13



I Driver:
Il nuovo Codice in materia di protezione dei dati personali
Decreto Legislativo 30 giugno 2003 n. 196

- Il nuovo Codice sulla Privacy, in armonizzazione con le garanzie contenute nella Carta del cittadino europeo, all'art. 1 ha introdotto nell'ordinamento il nuovo
Diritto alla protezione dei dati personali.
- ***L'importante principio riafferma un diritto della persona, più evidente rispetto al più generale diritto alla riservatezza presente nella precedente Legge, prima analizzata.***
- ***Sono molte le novità che hanno impatto sull'organizzazione e sugli strumenti elettronici, introdotte dal Nuovo Codice, tra esse la più importante è l'obbligatorietà di redigere un Documento Programmatico sulla Sicurezza e di riferire nella relazione accompagnatoria del bilancio d'esercizio dell'avvenuta redazione o dell'aggiornamento.***


Documento riservato - riproduzione anche parziale vietata 14 

I Driver:
Il nuovo Codice in materia di protezione dei dati personali
Decreto Legislativo 30 giugno 2003 n. 196

- **MISURE MINIME DI SICUREZZA**
Sicurezza dei trattamenti con strumenti elettronici
 - *Gli artt. dal 33 al 36 riproducono le previsioni dell'art. 15 c. 2 della Legge n. 675 del 31 dicembre 1996 e del d.P.R. 318/1999, ma apportano significativi miglioramenti di sicurezza.*

Le nuove norme, infatti, disciplinano la materia, evitando un'elencazione statica di misure puntuali, ed impostando una più attuale logica basata, per esempio, su standard di:

 - Autenticazione informatica;
 - Credenziali di autenticazione;
 - Sistema di Autenticazione;
 - Procedure di custodia di copie di sicurezza dei dati;
 - Procedure di ripristino dell'operatività;
 - Crittografia dei dati sensibili o giudiziari;
 - Aggiornamento dei sistemi, volti a prevenire vulnerabilità (es. le patch).

Documento riservato - riproduzione anche parziale vietata 15 

I Driver:
Il nuovo Codice in materia di protezione dei dati personali
Decreto Legislativo 30 giugno 2003 n. 196

■ **TRATTAMENTI CON STRUMENTI ELETTRONICI (Art. 34)**
 Il trattamento dei dati è quindi consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico (allegato B), le seguenti **misure minime**:

- a) **autenticazione informatica;**
- b) **adozione di procedure di gestione delle credenziali di autenticazione;**
- c) **utilizzo di un sistema di autorizzazione;**
- d) **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati ed addetti alla gestione o alla manutenzione degli strumenti elettronici;**
- e) **protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;**
- f) **adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;**
- g) **tenuta di un aggiornato documento programmatico sulla sicurezza;**
- h) **adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.**

A differenza del d.P.R. 318/1999 i trattamenti non vengono più distinti a seconda che siano eseguiti con elaboratori collegati in rete o non.

Tali misure minime di sicurezza sono comunque da adottare, ma con riferimento al quadro dei più generali obblighi di sicurezza di cui all'articolo n. 31, ovvero se previsti da speciali disposizioni.

Documento riservato - riproduzione anche parziale vietata

16

UniCredito Italiano

I Driver:
Il nuovo Codice in materia di protezione dei dati personali
Decreto Legislativo 30 giugno 2003 n. 196

■ **TRATTAMENTI CON STRUMENTI ELETTRONICI (Art. 34)**
 Il trattamento dei dati personali, effettuato con strumenti elettronici, deve inoltre risultare conforme al disciplinare tecnico contenuto nell'**Allegato B** al Decreto, composto da **26 regole**, da adottare a cura del **Titolare**, del **Responsabile** ove designato e dell'**Incaricato**.

Le **26 regole** disciplinano:

- Il sistema di autenticazione informatica;
- Il sistema di autorizzazione;
- Le altre misure di sicurezza;
- **Il Documento programmatico sulla sicurezza;**
- Le ulteriori misure in caso di trattamento di dati sensibili o giudiziari;
- Le misure di tutela e garanzia.

Documento riservato - riproduzione anche parziale vietata

17

UniCredito Italiano



I Driver:
Il nuovo Codice in materia di protezione dei dati personali
Decreto Legislativo 30 giugno 2003 n. 196

■ **II DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (Regola N. 19)**
Il Titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Entro il 31 marzo di ogni anno, il Titolare di un trattamento di **dati sensibili o di dati giudiziari** redige anche attraverso il responsabile, se designato, un *documento programmatico sulla sicurezza* contenente idonee informazioni riguardo:

Trattamenti con strumenti elettronici

1. l'**elenco dei trattamenti di dati personali**;
2. la distribuzione **dei compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati;
3. l'**analisi dei rischi che incombono sui dati**;
4. 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;
5. la descrizione di criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui alla regola 23 (Piano di **Disaster Recovery**);
6. 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 dal momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
7. 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;
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui alla Regola 24, l'individuazione dei criteri da adottare per la **cifatura** o per la separazione di tali dati dagli altri personali dell'interessato.

Documento riservato - riproduzione anche parziale vietata

18



LA SICUREZZA DELLE INFORMAZIONI: DA COSTO A VANTAGGIO COMPETITIVO



Da costo a vantaggio competitivo
Le **“Politiche generali di sicurezza delle informazioni”**

Necessità di avviare un piano organico della sicurezza delle informazioni capace di:

- coinvolgere tutte le “Business Units” dell’azienda;
- rispondere a requisiti internazionali di affidabilità e di gestione del rischio;
- contrastare le frodi e le attività criminali.


Necessità di rivedere la propria **struttura di governo della Privacy e della Sicurezza** facendo confluire su di un’unica funzione (quella della Security) la responsabilità dello **studio e dello sviluppo delle strategie, delle politiche e delle normative in tema di sicurezza**, garantendo in tal modo uniformità di indirizzo in una così delicata materia.

Le Politiche generali di sicurezza o **“policies”** costituiscono il primo importante obiettivo di allineamento ad una base comune di sicurezza per tutelare uniformemente il patrimonio aziendale ed i sistemi informativi e telematici da attacchi e/o alterazioni, comprese le frodi informatiche.

Documento riservato – riproduzione anche parziale vietata

20





Da costo a vantaggio competitivo
Le **“Politiche generali di sicurezza delle informazioni”**


La redazione delle “policies”, basata sulle ormai famose BS/7799 e ISO/IEC 17799:2000, hanno consentito di censire tutti i rischi e di “normare” gli aspetti di protezione delle informazioni, in particolare:

- **La Sicurezza Fisica;**
- **La Sicurezza Logica;**
- **La Sicurezza delle reti di telecomunicazioni;**
- **La firma digitale;**
- **La Sicurezza dei server e dei siti web;**
- **La gestione degli incidenti;**
- **La Sicurezza organizzativa;**
- **Il piano di continuità operativa;**
- **La verifiche;**
- **Le norme operative;**

costituendo così una “revisione critica” di tutti i processi di business.

Documento riservato – riproduzione anche parziale vietata

21



Da costo a vantaggio competitivo Un esempio di revisione critica del processo: I Sistemi Biometrici in architettura PKI

Rilevazione Biometrica - Architettura di sicurezza

Le immagini e le impronte sono crittografate con una chiave segreta simmetrica, avente lunghezza minima di 128 bit... Tale chiave viene successivamente crittografata con la chiave pubblica recuperata dal certificato X509 v3 memorizzato nel sistema biometrico.

L'impronta è acquisita rispettando gli standard e le specifiche AFIS.

L'accesso allo sportello avviene su base volontaria e consensuale con un solo gesto dell'Interessato.

E' possibile entrare con altre modalità nei locali, tramite il Responsabile dello sportello.

Il Sistema è ad altissima sicurezza in quanto nell'elaboratore di gestione non sono mai memorizzate le chiavi segrete di decrittazione, presenti solo su smart card IT/SEC protette da apposita password (PIN).

Tramite la chiave segreta presente solo nella smart card, l'Autorità Giudiziaria potrà decrittare le impronte e le immagini e scaricare le medesime in formato AFIS.

Documento riservato - riproduzione anche parziale vietata

22

Da costo a vantaggio competitivo Un esempio di revisione critica del processo: I Sistemi Biometrici in architettura PKI

Il processo di cifratura

Archivio pronto delle impronte e delle chiavi simmetriche cifrate

Il processo di decifratura

Impronta decrittata in chiaro


Documento riservato - riproduzione anche parziale vietata

23

Da costo a vantaggio competitivo
Un esempio di revisione critica del processo:
I Sistemi Biometrici in architettura PKI: I Vantaggi

- Impossibilità "tecnica" per il personale di accedere ai dati crittografati;
- Disponibilità delle più aggiornate e sofisticate tecnologie di sicurezza (chip ITSEC);
- L'hardware dei sistemi attualmente installati viene mantenuto invariato, con la sola aggiunta di un lettore di smart card avente un costo di circa 30 €;
- La crittografia asimmetrica consente di utilizzare i sistemi, con la massima sicurezza oggi disponibile, anche su reti disponibili al pubblico, assicurando alle banche benefici economici e gestionali (aggiornamenti centralizzati degli antivirus, installazione di patch di Sistema Operativo che ora sono imposte dal nuovo Codice sulla Privacy, ecc.);
- L'architettura consente di essere compatibili con l'utilizzo di carte di identità elettroniche basate su certificati X.509 v3;
- Non sono più necessari interventi di personale specializzato presso le Filiali, che attualmente rappresentano il problema di sicurezza maggiore e l'onere economico principale dei sistemi finora installati.

24



Da costo a vantaggio competitivo
In sintesi ...

Documento programmatico sulla sicurezza (D. Lsg. 196/2003)
Modello organizzativo e procedurale (D. Lsg. 231/2001)

<u>FIRMA DIGITALE SMART CARD</u>	<u>EFS CONTROLLO ACCESSI BIOMETRICI</u>	<u>ANTIVIRUS FIREWALL BACK-UP DISASTER RECOVERY</u>	
--	---	---	--

**Sicurezza idonea =
Vantaggio competitivo**

**Politiche di
sicurezza delle
informazioni**

**Analisi dei rischi e
classificazione delle
informazioni**

25



LE NUOVE TECNOLOGIE

Le Tecnologie
Le tecnologie devono sempre tenere conto di tutte le esigenze

Documento riservato – riproduzione anche parziale vietata

27

UniCredito Italiano

Le Tecnologie
Come proteggere le informazioni ed i sistemi?

Come proteggere quindi le informazioni?

- **Attribuire un valore alle proprie informazioni** individuando quelle critiche attraverso **un'analisi dei rischi e delle vulnerabilità.**
- **Classificare le informazioni**, attribuendo loro un grado di riservatezza, al quale corrisponde una maggiore o minore circolazione all'interno ed all'esterno dell'azienda.
- **Riservare livelli crescenti di protezione solo alle informazioni che lo richiedano per loro natura**, dato che l'onere della protezione può risultare elevato.

Viene definita una priorità in termini di sicurezza

Documento riservato – riproduzione anche parziale vietata

28

UniCredito Italiano

Le Tecnologie
Come proteggere le informazioni ed i sistemi?

Le misure di sicurezza sono state da noi sviluppate secondo tre principi base:



1. **L'integrità:** intesa come la gestione dell'accuratezza e della completezza delle informazioni, la salvaguardia dei dati, l'esattezza e la difesa da manomissioni ovvero modifiche non autorizzate;
2. **La confidenzialità:** cioè la garanzia che le informazioni siano accessibili solo alle persone e entità autorizzati, la protezione delle linee di trasmissione dei dati, il controllo logico e fisico degli accessi;
3. **La disponibilità:** intesa come l'assicurazione che l'accesso ai dati sia disponibile quando necessario, quindi la garanzia per gli utenti della fruibilità dei dati e dei servizi.

Documento riservato - riproduzione anche parziale vietata

29




Le Tecnologie
Alcuni dei sistemi di sicurezza adottati

- La **firma digitale** applicata ai file trasmessi al Registro delle Imprese, ai messaggi di posta elettronica, ai file critici dei Sistemi Operativi adottati, all'interscambio interno di file riservati.
- I **security chip RSA** integrati nei notebook, che consentono di memorizzare ogni password utilizzata dall'Utente in un chip ad alta sicurezza, integrato nella scheda di sistema.
- I **Crypto File System** (come l'EFS di Windows 2000 o XP).
- I **Firewall integrati** nei S.O. Windows XP o Windows Server 2003.
- I **Firewall e gli Intrusion Detection**, integrati nella suite Antivirus Norton Symantec che viene installata in ogni PC critico.
- Gli **Antivirus aggiornati on-line**, in modalità non presidiata, aventi i file di aggiornamento "firmati" elettronicamente dal fornitore.
- **Smart card** ad alta sicurezza.
- Strumenti di verifica automatica della sicurezza, come p.e. **Microsoft Baseline Security Analyzer**, installati nei client o gruppi di client critici.
- I **chip RFID (Radio-Frequency Identification)** con motore RSA per la gestione di badge nel controllo accessi evoluto.

Documento riservato - riproduzione anche parziale vietata

30



Le Tecnologie La Firma Digitale

- E' stata adottata la firma digitale, conforme alle disposizioni di legge in materia e certificata da primaria Certification Authority Italiana.
- La U.O. Sicurezza di Gruppo ha assunto il ruolo ufficiale di Registration Authority.
- Sono stati inoltre adottati i migliori sistemi software di firma digitale, che consentono l'utilizzo della firma a valore legale anche per altre procedure automatizzate, come l'interscambio sicuro di file o di e-mail.

DOCUMENTO → Messaggio di Digest → MESSAGGIO DIGEST

MESSAGGIO DIGEST → Messaggio di Digest + Chiave Privata → FIRMA

La firma digitale qualificata, conforme alle più rigide disposizioni di Legge

31

Documento riservato – riproduzione anche parziale vietata

UniCredito Italiano

Le Tecnologie Gli standard adottati

- I principali standard adottati, per le applicazioni di sicurezza, si riferiscono a quanto disponibile e tecnicamente riconosciuto attualmente a livello internazionale:
 - Algoritmo di crittografia a chiave pubblica: **RSA, con chiavi di lunghezza minima pari a 1024 bit;**
 - Algoritmi di crittografia a chiave simmetrica: **3DES** o DES;
 - Algoritmo di HASH: **SHA-1** (FIPS PUB 180-1);
 - Algoritmo di firma digitale: **SHA1** con RSA e padding PKCS#1;
 - Formato dei certificati: ITU-T **X509 v3** (ISO/IEC 9594-8);
 - Formato delle richieste di certificato: **PKCS#10** (RFC 2314);
 - Formato delle buste crittografiche: **PKCS#7** (RFC 2315);
 - Interfacciamento con la smartcard: **PKCS#11 v2.0;**
 - Comunicazione con il lettore di smartcard: **PC/SC;**
 - Formato di import/export credenziali: **PKCS#12;**
 - Algoritmo di cifratura della chiave privata su file system: **3DES** e **RSA;**
 - Protocollo di accesso alla directory: **LDAP v3** (RFC 2251);
 - Algoritmo di validazione di catene di certificati: conforme a **RFC 2459**

32

Documento riservato – riproduzione anche parziale vietata

UniCredito Italiano

Le Tecnologie

La Firma Digitale applicata ai file

Il file system EFS (Encrypting File System)

- Microsoft ha dato notevole importanza alla sicurezza delle informazioni, nella realizzazione dei nuovi Sistemi Operativi.
- L'EFS è ora presente in tutti i S.O. di Microsoft dalla release 2000 a Windows XP ovvero 2003.
- L'operazione è del tutto trasparente all'utente ed estremamente sicura (soprattutto per i notebook).

Documento riservato – riproduzione anche parziale vietata

33

Le Tecnologie

Gli Antivirus ed i Firewall integrati

- Abbiamo ritenuto indispensabile disporre di sofisticati sistemi antivirus che eseguano un completo controllo di ogni operazione eseguita dall'utente, sia se connesso alla rete interna (LAN), geografica (WAN) ovvero a Internet.
- Si ritiene inoltre necessario dotare i Client critici di **Firewall e di Intrusion Detection** sia a livello di server, ed altri PC qualora il tipo di dati trattati (es.: dati *sensibili* o *price sensitive*), ovvero l'operatività lo giustifichi.

Documento riservato – riproduzione anche parziale vietata

34

Le Tecnologie
I processi di autenticazione adottati

I nuovi sistemi di autenticazione, conformi al disciplinare tecnico (allegato B) del D. Lgs. 196/2003, possono essere basati su:

Firma digitale	Crittografia
Certificati X.509 v3	Caratteristica Biometrica

- **Firma digitale** delle password o dei certificati;
- **Smart card** ad alta sicurezza;
- Chip **RFID** con PIN, integrati nei badge in dotazione al Personale;
- Architetture **PKI** con Certification Authority interne;
- **Caratteristiche biometriche dell'Utente**, come l'impronta dattiloscopica (template dell'impronta digitale, ottenuto con un algoritmo irreversibile, come lo SHA-1).

Documento riservato - riproduzione anche parziale vietata

35

