

SICUREZZA INFORMATICA

**IL CRESCENTE RICORSO ALLE TECNOLOGIE
DELL'INFORMAZIONE E DELLA COMUNICAZIONE INTRAPRESO
DALLA P.A. PER**

- **LO SNELLIMENTO**
- **L'OTTIMIZZAZIONE**
- **UNA MAGGIORE EFFICIENZA**

DEI PROCEDIMENTI AMMINISTRATIVI

COMPORTA UNA SERIE DI “NUOVI” RISCHI

***RISCHI CHE, SE NON ADEGUATAMENTE AFFRONTATI,
POTREBBERO COMPORTARE***

GRAVI CONSEGUENZE

SULL'AFFIDABILITÀ DEI DATI E DEI SERVIZI

I RISCHI “INFORMATICI” SONO IMPUTABILI A DUE FATTORI CARATTERISTICI DELLA TECNOLOGIA IN QUESTIONE:

- ***INAFFIDABILITÀ*** NON GARANZIA DI CORRETTO FUNZIONAMENTO SIA NELLE COMPONENTI HARDWARE SIA IN QUELLE SOFTWARE
- ESPOSIZIONE ALLE ***INTRUSIONI INFORMATICHE***

***LA SICUREZZA DEL SISTEMA INFORMATIVO AUTOMATIZZATO
NON DIPENDE SOLO DA ASPETTI TECNICI, MA ANCHE DA
QUELLI:***

- **ORGANIZZATIVI**
- **SOCIALI**
- **LEGALI**

VIENE DEFINITO SICURO UN SISTEMA INFORMATIVO AUTOMATIZZATO CHE SODDISFI LE SEGUENTI PROPRIETÀ:

- **DISPONIBILITÀ**
- **INTEGRITÀ**
- **AUTENTICITÀ**
- **CONFIDENZIALITÀ O RISERVATEZZA**

DISPONIBILITÀ

***L'INFORMAZIONE ED I SERVIZI DEVONO ESSERE A
DISPOSIZIONE DEGLI UTENTI DEL SISTEMA COMPATIBILMENTE
CON I LIVELLI DI SERVIZIO***

INTEGRITÀ

L'INFORMAZIONE ED I SERVIZI EROGATI POSSONO ESSERE CREATI, MODIFICATI O CANCELLATI SOLO ALLE PERSONE AUTORIZZATE A SVOLGERE TALE OPERAZIONE

AUTENTICITA'

GARANZIA E CERTIFICAZIONE DELLA PROVENIENZA DEI DATI

CONFIDENZIALITÀ O RISERVATEZZA

***L'INFORMAZIONE PUÒ ESSERE FRUITA SOLO DALLE PERSONE
AUTORIZZATE***

***L 'ADOZIONE DELLE CONTROMISURE PER PREVENIRE O
RIDURRE IL RISCHIO INFORMATICO***

***NON È LASCIATA ALLA DISCREZIONE DELLE SINGOLE
AMMINISTRAZIONI***

MA

È UN OBBLIGO DI LEGGE

ARCHITETTURA DI SICUREZZA

E' L'INSIEME DI

- ***REGOLE***
- ***FUNZIONI***
- ***STRUMENTI***
- ***OGGETTI***
- ***CONTROLLI***

COERENTEMENTE DISEGNATI E RESI FUNZIONANTI, CHE GARANTISCONO IL RISPETTO DEGLI STANDARD DI SICUREZZA DEFINITI DALL'AMMINISTRAZIONE O DALLA LEGGE

L'ARCHITETTURA DI SICUREZZA SI "APPLICA" IN OGNI SITUAZIONE SOGGETTA A RISCHIO INFORMATICO

- **STRUTTURA ORGANIZZATIVA**
- **AMBIENTE INFORMATICO**
- **SISTEMA INFORMATIVO**
- **SINGOLO ELABORATORE**

GLI ELEMENTI ESSENZIALI DI UNA ARCHITETTURA DI SICUREZZA SONO:

FUNZIONI DI SICUREZZA

IDENTIFICAZIONE E AUTENTICAZIONE DEGLI UTENTI, CONTROLLO ACCESSI AI DATI ED ALLE APPLICAZIONI, CRITTOGRAFIA, NON RIGETTO, FIRMA ELETTRONICA, ECC.

MECCANISMI DI SICUREZZA

SONO I PRODOTTI HARDWARE E SOFTWARE CHE REALIZZANO LE FUNZIONI DI SICUREZZA PREVISTE NELL'ARCHITETTURA.

OGGETTI DI SICUREZZA

FANNO PARTE DI QUESTA CATEGORIA LE PASSWORD, LE CHIAVI DI CRITTOGRAFIA, LE LISTE DI ACCESSO, ECC. .UNA PROTEZIONE NON APPROPRIATA DI QUESTI OGGETTI POTREBBE VANIFICARE L'EFFICACIA DELL'INTERO SISTEMA.

PROCESSI DI GESTIONE (PROCEDURE)

E' L'INSIEME DEI PROCESSI E DELLE REGOLE PER LA GESTIONE DELLE FUNZIONI, DEI MECCANISMI E DEGLI OGGETTI DI SICUREZZA CHE FANNO PARTE DELLA ARCHITETTURA. VI DOVREBBERO FAR PARTE ANCHE PROCESSI DI ALLARME E CONTROLLO.

LE ATTIVITÀ DI SVILUPPO DI UN PIANO DI .SICUREZZA SONO RIFERITE ALLE SEGUENTI AREE:

- **SICUREZZA FISICA**
- **SICUREZZA LOGICA**
- **SICUREZZA ORGANIZZATIVA**
- **PIANO DI CONTINUITÀ OPERATIVA**

SICUREZZA FISICA

- **PROTEGGERE LE PERSONE CHE OPERANO SUI SISTEMI**
- **PROTEGGERE LE AREE**
- **PROTEGGERE LE COMPONENTI DEL SISTEMA INFORMATIVO**

SICUREZZA FISICA

SICUREZZA DI AREA

OBIETTIVO

PREVENIRE ACCESSI FISICI NON AUTORIZZATI DANNI O INTERFERENZE CON LO SVOLGIMENTO DEI SERVIZI

CONSISTE IN

- **PROTEZIONI PERIMETRALI DEI SITI**
- **CONTROLLI FISICI ALL'ACCESSO**
- **SICUREZZA DEI LOCALI DOVE SONO I COMPUTER RISPETTO A DANNEGGIAMENTI**
- **PROTEZIONE FISICA DEI SUPPORTI**

SICUREZZA FISICA

SICUREZZA DELLE APPARECCHIATURE HARDWARE

OBIETTIVI

- **PROTEZIONI DA DANNEGGIAMENTI**
- **SICUREZZA DEGLI IMPIANTI DI ALIMENTAZIONE E DI CONDIZIONAMENTO**
- **MANUTENZIONE DELL'HARDWARE**
- **PROTEZIONE DA MANOMISSIONE O FURTI**

SICUREZZA LOGICA

PROTEZIONE

- **DELL'INFORMAZIONE**
- **DEI DATI**
- **DELLE APPLICAZIONI**
- **DEI SISTEMI**
- **DELLE RETI**

SICUREZZA LOGICA

SI ARTICOLA IN MISURE DI SICUREZZA

- **DI CARATTERE TECNOLOGICO**
- **DI NATURA PROCEDURALE E ORGANIZZATIVA**

LA REALIZZAZIONE DELLA SICUREZZA LOGICA DEVE ESSERE PENSATA IN TERMINI ARCHITETTURALI

LA DEFINIZIONE DELL'ARCHITETTURA DI SICUREZZA LOGICA DEVE RISPONDERE ALLE SEGUENTI DOMANDE:

QUALI FUNZIONI DI SICUREZZA DEVONO ESSERE GARANTITE E PER QUALI BENI ?

CON QUALI MECCANISMI DI SICUREZZA È CONVENIENTE REALIZZARE TALI FUNZIONI ?

IN QUALI LIVELLI DELL'ARCHITETTURA DEL SISTEMA INFORMATICO DEVONO ESSERE COLLOCATI I DIVERSI MECCANISMI?

LA REALIZZAZIONE DELL'ARCHITETTURA DI SICUREZZA SI BASA SULL'INDIVIDUAZIONE DI:

- **SERVIZI DI SICUREZZA**
- **MECCANISMI DI SICUREZZA**
- **FUNZIONI DI SICUREZZA**

CHE IL SISTEMA DOVRÀ GARANTIRE SU TUTTE LE PIATTAFORME ED A TUTTI I LIVELLI DI ELABORAZIONE.

LE NORME ISO INDIVIDANO, FRA GLI ALTRI, I SEGUENTI SERVIZI DI SICUREZZA :

- **AUTENTICAZIONE**
- **CONTROLLO ACCESSI**
- **CONFIDENZIALITÀ**
- **INTEGRITÀ**
- **NON RIPUDIO**

MECCANISMI DI SICUREZZA

**MODALITÀ TECNICHE ATTRAVERSO LE QUALI È POSSIBILE
REALIZZARE I SERVIZI DI SICUREZZA**

ISO INDIVIDUA I SEGUENTI MECCANISMI DI SICUREZZA :

- **CIFRATURA**
- **FIRMA DIGITALE**
- **MECCANISMI PER IL CONTROLLO DEGLI ACCESSI INTEGRITÀ DEI DATI**
- **MECCANISMI PER L'AUTENTICAZIONE**

SICUREZZA ORGANIZZATIVA

NORME E PROCEDURE MIRANTI A REGOLAMENTARE GLI ASPETTI ORGANIZZATIVI DEL PROCESSO DELLA SICUREZZA

SICUREZZA ORGANIZZATIVA

- **DEFINIZIONE DI RUOLI, COMPITI E RESPONSABILITÀ ,PER LA GESTIONE DI TUTTE LE FASI DEL PROCESSO DI SICUREZZA**
- **ADOZIONE DI SPECIFICHE PROCEDURE CHE VADANO A COMPLETARE E RAFFORZARE LE CONTROMISURE TECNOLOGICHE ADOTTATE**
- **CONTROLLI SULLA CONSISTENZA E SULLA AFFIDABILITÀ DEGLI APPARATI**

PIANO DI CONTINUITA OPERATIVA

- **RIPRISTINARE I SERVIZI INFORMATICI IN CASO DI INTERRUZIONE**
- **RENDERE MINIME LE PERDITE CAUSATE DALL'INTERRUZIONE DELL'ATTIVITÀ**

ANALISI DEI RISCHI

I RISCHI SI POSSONO CLASSIFICARE SECONDO L'ORIGINE

INTERNI	CONNESSI ALLA ATTIVITÀ DEI DIPENDENTI DELLA AMMINISTRAZIONE (SECONDO LE STATISTICHE SONO I PIÙ PROBABILI)
ESTERNI	CONNESSI ALLA ATTIVITÀ DI QUALUNQUE ALTRA PERSONA.
AMBIENTALI	RELATIVI A EVENTI DI GRANDE PORTATA, QUALI: INCENDI, TERREMOTI, ALLAGAMENTI, ECC.

ANALISI DEI RISCHI

I RISCHI SI POSSONO CLASSIFICARE SECONDO LE CAUSE

**CARENZE
ORGANIZZATIVE**

RESPONSABILITÀ NON CORRETTAMENTE
ASSEGNATE, SOTTOVALUTAZIONE DEI RISCHI,
ECC. .

COLPA

SE CAUSATI DA IGNORANZA, INCURIA O
LEGGEREZZA

DOLO

IN RAPIDA CRESCITA

ANALISI DEI RISCHI

I RISCHI SI POSSONO CLASSIFICARE SECONDO LE MODALITA'

INTERCETTAZIONI	PRINCIPALMENTE LUNGO LA RETE DI TRASMISSIONE
INGEGNERIA SOCIALE	PER DIVERTIMENTO, SI PRENDE GIOCO DELLA VITTIMA (SONO LE MODALITÀ PIÙ DIFFUSE E PERICOLOSE)
BACKDOOR	QUANDO I PROGRAMMATORI LASCIANO DEI PUNTI DI INGRESSO NON NOTI NEL SOFTWARE
CAVALLI DI TROIA	SOFTWARE PREDISPOSTO PER OPERARE IN MODO NON NOTO ALL'UTENTE

ANALISI DEI RISCHI

I RISCHI SI POSSONO CLASSIFICARE SECONDO LE MODALITA'

DENIAL OF SERVICE	COMANDI CHE PREGIUDICANO LA EFFICIENZA DELLE RETI E DEI SERVER
VIRUS	SOFTWARE CHE HA LA CAPACITÀ DI AUTOPROPAGARSI
PERSONIFICAZIONE	QUANDO CI SI PRESENTA SOTTO MENTITE SPOGLIE

LA LISTA POTREBBE ESSERE PIÙ LUNGA. CON L'AVVENTO DELL'INFORMATICA DISTRIBUITA E DI INTERNET, IL POSSIBILE HACKER PUÒ ESSERE CHIUNQUE E IN QUALUNQUE PARTE DEL MONDO ED È PRATICAMENTE IMPOSSIBILE INDIVIDUARLO

CHE FARE?

**INTRODUZIONE E DIFFUSIONE DELLA CULTURA DELLA
SICUREZZA INFORMATICA NELLA PUBBLICA
AMMINISTRAZIONE**

**ASSICURARE LA MIGLIOR SICUREZZA DEI SISTEMI
INFORMATIVI AUTOMATIZZATI PRESENTA PARTICOLARI
PROBLEMATICHE D'ORDINE**

- **CULTURALE**
- **SOCIALE**
- **ORGANIZZATIVO**
- **LEGALE**
- **TECNICO**

È QUINDI NECESSARIO ELABORARE ED ATTUARE SPECIFICHE STRATEGIE DI

- **SENSIBILIZZAZIONE**
- **CORRESPONSABILIZZAZIONE**
- **FORMAZIONE**