STITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO S.I.A. Sistemi Informativi Automatizzati	**ANALISI DEI RISCHI PROGETTO ISMS** **EXECUTIVE SUMMARY** **Ambito: SIA** **Data: 14/12/2007** **Rapporto N.: 200701**	Rev. 1 Pag.14 /22 ***Riservato***

[SOWIN.SOW2] Sistema Operativo WINXP	{4}		
[SOWIN.EXC] EXCHANGE server 2003	{4}		
[SOLIN] Red Hat per DNS	{3}		
[Tec.Cond] Condizionatori/Distribuzione	{2}		
[Tec.Alim] Alimentazione primaria/cablaggio/UPS/Elettrogeni	{2}		
[Tec.ARM] Armadi di rack - Ignifughi	{1}		
[Ntec.App] Approvigionamenti essenziali	{1}		
[Ntec.Cas] Casseforti	{1}		
[Ntec.Adis] Apparati di distruzione supporti	{2}		
[RBK] Robot Backup su nastro	{3}		
[DC.CTRb] Contabilità di bilancio	{3}	{3}	{4}
[DC.CTRd] Contratti di lavoro dipendenti	{3}	{3}	{3}
[DC.CTRf] Contratti Fornitori	{3}	{3}	{3}
[DC.CTRc] Contratti Clienti	{3}	{3}	{3}
[PA.RSC] Dati Ricerca - Documentazione tecnica	{3}	{3}	
[PA.OMC] Dati Omologazione, Certificazione e 626/94	{4}	{3}	
[PA.DTEP] Dati Sicurezza sul Lavoro - EPIDEMIOLOGICI E PREVENZIONE INFORTUNI	{3}	{3}	
[DPr.DP] Dati Personali - 196/03	{3}	{2}	{3}
[DPr.DS] Dati Sensibili e Giudiziari - 196/03	{4}	{3}	{4}
[DT.LOG] Log	{4}	{3}	{4}
[DT.DHDK] Dati Help Desk	{3}	{2}	
[DT.DBCK] Dati Backup	{4}	{3}	{4}
[DT.DTC] Dati tecnici Ced	{4}	{4}	{4}
[uff] Uffici	{1}		
[LCED] CED	{2}		
[EDI] Edificio			

STITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO S.I.A. Sistemi Informativi Automatizzati	**ANALISI DEI RISCHI PROGETTO ISMS** **EXECUTIVE SUMMARY** **Ambito: SIA** **Data: 14/12/2007** **Rapporto N.: 200701**	Rev. 1 Pag.15 /22 ***Riservato***

Situazione a medio

asset	[D]	[I]	[R]
[PDL2.PDLA] Posto di lavoro Amministrativi	(1)		
[PDL2.PDLT] Posto di Lavoro Tecnici	(1)		
[AUFF] Sever di Piano per File sharing - 1,7 piani	(1)		
[Area SAS] 2 Server SAS del DPO	(1)		
[CED.DMZ.DMZ RAS] Server RAS - Remote Access Server	(1)		
[CED.DMZ.DMZ Net] Server Proxy (ISA)/Server DNS	(1)		
[CED.DMZ.DMZ WEB] Server Web/Inf Mortali (DPO)/VSR-VSG (DCC)	(1)		
[CED.DMZ.DMZ Apparati di rete] Switch / Firewall	(1)		
[CED.LN.CLEX] CLUSTER EXCHANGE 2fe+2be+1SAN	(1)		
[CED.LN.CL2.SNET] Server di Rete DHCP/File Sharing/Print Sharing	(1)		
[CED.LN.CL2.SQL] SQL 2005	(1)		
[CED.LN.SAN] Storage Area Network	(1)		
[CED.LN.SRV DC] 2 SERVER DI DOMAIN CONTROLLER+WSUS	(1)		
[CED.LN.TS] TERMINAL SERVER	(1)		
[CED.LN.BCK] SERVER BACKUP	(1)		
[CED.LN.ORL] SERVER ORACLE per DML	(1)		
[CED.LN.MNG] SERVER ANTIVIRUS ED HELP DESK	(1)		
[CED.LN.SW] SERVER DI SVILUPPO WEB	(1)		
[WAN] Switch WAN/VPN Concentrator	(1)		
[LAN] LAN Via Alessandria	(1)		
[UCED.AS] AMMINISTRATORI SISTEMA	(2)		
[UCED.OShd] OPERATORE HELP DESK	(2)		
[UCED.EXT] PERSONALE ESTERNO	(2)		
[PEXT2.EXT2] Personale esterno al CED	(1)		
[UA.PU] PERSONALE AMMINISTRATIVO UTENTE	(2)		
[Appl] Software applicativo - installato di base sui pc	(2)		
[Base.BKP] ARCSERVE BRIGTSTORE BACKUP	(2)		
[Base.ORC] Oracle	(2)		
[Base.DB] SQL 2005	(2)		
[OCWIN Sowl Windows server 2003	(2)		

ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO S.I.A. Sistemi Informativi Automatizzati	**ANALISI DEI RISCHI** **PROGETTO ISMS** **EXECUTIVE SUMMARY** **Ambito: SIA** **Data: 14/12/2007** **Rapporto N.: 200701**	Rev. 1 Pag.16 /22 ***Riservato***

[SOWIN.SOW2] Sistema Operativo WINXP	(2)		
[SOWIN.EXC] EXCHANGE server 2003	(2)		
[SOLIN] Red Hat per DNS	(2)		
[Tec.Cond] Condizionatori/Distribuzione	(1)		
[Tec.Alim] Alimentazione primaria/cablaggio/UPS/Elettrogeni	(1)		
[Tec.ARM] Armadi di rack - Ignifughi	(0)		
[Ntec.App] Approvigionamenti essenziali	(0)		
[Ntec.Cas] Casseforti	(1)		
[Ntec.Adis] Apparati di distruzione supporti	(1)		
[RBK] Robot backup su nastro	(2)		
[DC.CTRb] contabilità di bilancio	(2)	(2)	(2)
[DC.CTRd] Contratti di lavoro dipendenti	(2)	(2)	(2)
[DC.CTRf] Contratti Fornitori	(2)	(2)	(2)
[DC.CTRc] Contratti Clienti	(2)	(2)	(2)
[PA.RSC] Dati Ricerca - Documentazione tecnica	(2)	(2)	
[PA.OMC] Dati Omologazione, Certificazione e 626/94	(2)	(2)	
[PA.DTEP] Dati Sicurezza sul Lavoro - EPIDEMIOLOGICI E PREVENZIONE INFORTUNI	(2)	(2)	
[DPr DP] Dati Personali - 196/03	(2)	(2)	(2)
[DPr.DS] Dati Sensibili e Giudiziari - 196/03	(2)	(2)	(2)
[DT.LOG] Log	(2)	(2)	(2)
[DT.DHDK] Dati Help Desk	(2)	(1)	
[DT.DBCK] Dati Backup	(2)	(2)	(2)
[DT.DTC] Dati tecnici Ced	(2)	(2)	(2)
[uff] Uffici	(1)		
[LCED] CED	(1)		
[EDI] Edificio	(0)		

ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO S.I.A. Sistemi Informativi Automatizzati	ANALISI DEI RISCHI PROGETTO ISMS EXECUTIVE SUMMARY Ambito: SIA Data: 14/12/2007 Rapporto N.: 200701	Rev. 1 Pag.17 /22 ***Riservato***

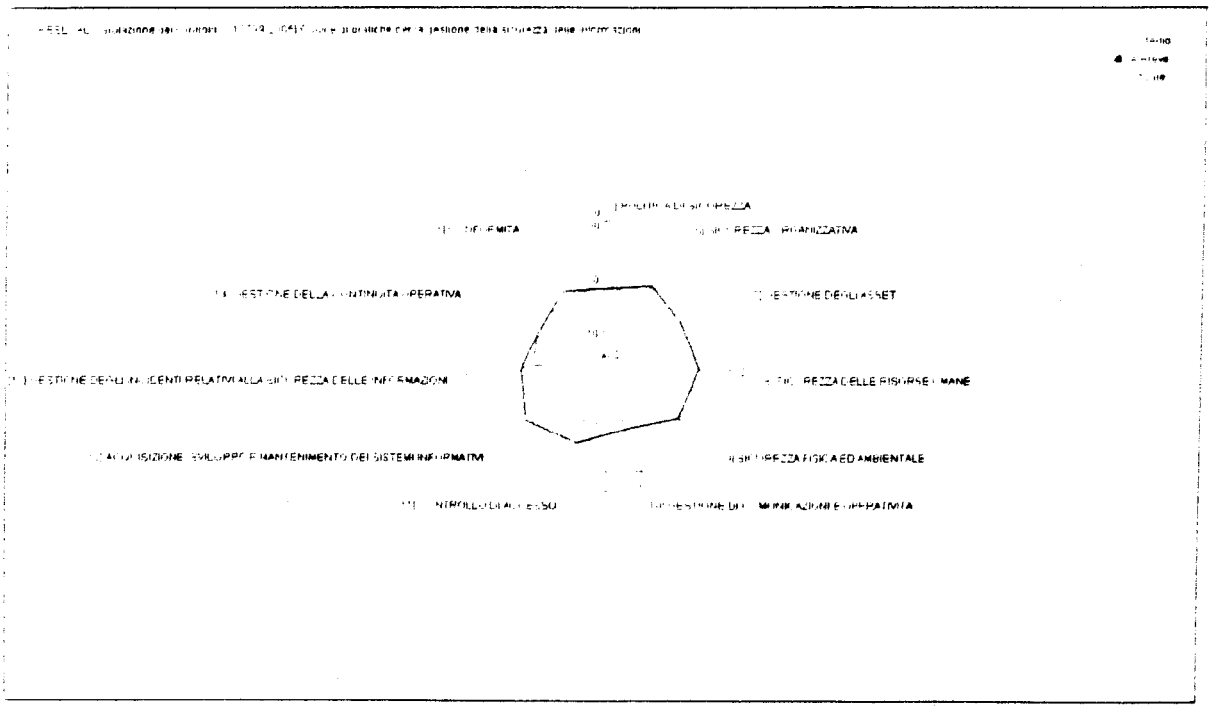
Evoluzione per la disponibilità

asset	potenziale	Attuale	A Breve	A Medio
[PDL2.PDLA] Posto di lavoro Amministrativi	{5}	{4}	{2}	{1}
[PDL2.PDLT] Posto di Lavoro Tecnici	{5}	{4}	{2}	{1}
[AUFF] Sever di Piano per File sharing - 1,7 piani	{5}	{5}	{3}	{1}
[Area SAS] 2 Server SAS del DPO	{5}	{5}	{3}	{1}
[CED.DMZ.DMZ RAS] Server RAS - Remote Access Server	{3}	{3}	{2}	{1}
[CED.DMZ.DMZ Net] Server Proxy (ISA)/Server DNS	{5}	{5}	{3}	{1}
[CED.DMZ.DMZ WEB] Server Web/Inf Mortali (DPC)/VSR-VSG (DCC)	{5}	{5}	{3}	{1}
[CED.DMZ.DMZ Apparati di rete] Switch / Firewall	{5}	{5}	{3}	{1}
[CED.LN.CLEX] CLUSTER EXCHANGE 2fe+2be+1SAN	{5}	{5}	{3}	{1}
[CED.LN.CL2.SNET] Server di Rete DHCP/File Sharing/Print Sharing	{5}	{5}	{3}	{1}
[CED.LN.CL2.SQL] SQL 2005	{5}	{5}	{3}	{1}
[CED.LN.SAN] Storage Area Network	{5}	{5}	{3}	{1}
[CED.LN.SRV DC] 2 SERVER DI DOMAIN CONTROLLER+WSUS	{5}	{5}	{3}	{1}
[CED.LN.TS] TERMINAL SERVER	{5}	{4}	{2}	{1}
[CED.LN.BCK] SERVER BACKUP	{5}	{4}	{2}	{1}
[CED.LN.ORL] SERVER ORACLE per DML	{5}	{4}	{2}	{1}
[CED.LN.MNG] SERVER ANTIVIRUS ED HELP DESK	{5}	{5}	{3}	{1}
[CED.LN.SW] SERVER DI SVILUPPO WEB	{3}	{3}	{2}	{1}
[WAN] Switch WAN/VPN Concentrator	{5}	{4}	{2}	{1}
[LAN] LAN Via Alessandria	{5}	{5}	{3}	{1}
[UCED.AS] AMMINISTRATORI SISTEMA	{5}	{5}	{4}	{2}
[UCED.OShd] OPERATORE HELP DESK	{5}	{4}	{3}	{2}
[UCED.EXT] PERSONALE ESTERNO	{5}	{5}	{4}	{2}
[PEXT2.EXT2] Personale esterno al CED	{4}	{3}	{1}	{1}
[UA.PU] PERSONALE AMMINISTRATIVO UTENTE	{5}	{4}	{3}	{2}
[Appl] Software applicativo - installato di base sui pc	{5}	{5}	{4}	{2}
[Base.BKP] ARCSERVE BRIGTSTORE BACKUP	{5}	{4}	{3}	{2}
[Base.ORC] Oracle	{5}	{4}	{3}	{2}
[Base.DB] SQL 2005	{5}	{5}	{4}	{2}

[SOWIN.Sow] Windows server 2003	{5}	{5}	{5}	{2}
[SOWIN.SOW2] Sistema Operativo WINXP	{5}	{5}	{4}	{2}
[SOWIN.EXC] EXCHANGE server 2003	{5}	{5}	{4}	{2}
[SOLIN] Red Hat per DNS	{5}	{5}	{3}	{2}
[Tec.Cond] Condizionatori/Distribuzione	{4}	{3}	{2}	{1}
[Tec.Alim] Alimentazione primaria/cablaggio/UPS/Elettrogeni	{5}	{4}	{2}	{1}
[Tec.ARM] Armadi di rack - Ignifughi	{3}	{2}	{1}	{0}
[Ntec.App] Approvigionamenti essenziali	{3}	{2}	{1}	{0}
[Ntec.Cas] Casseforti	{4}	{3}	{1}	{1}
[Ntec.Adis] Apparati di distruzione supporti	{4}	{3}	{2}	{1}
[RBK] Robot backup su nastro	{5}	{4}	{3}	{2}
[DC.CTRb] contabilità di bilancio	{5}	{5}	{3}	{2}
[DC.CTRd] Contratti di lavoro dipendenti	{5}	{5}	{3}	{2}
[DC.CTRf] Contratti Fornitori	{5}	{5}	{3}	{2}
[DC.CTRc] Contratti Clienti	{5}	{5}	{3}	{2}
[PA.RSC] Dati Ricerca - Documentazione tecnica	{5}	{5}	{3}	{2}
[PA.OMC] Dati Omologazione, Certificazione e 626/94	{5}	{5}	{4}	{2}
[PA.DTEP] Dati Sicurezza sul Lavoro - EPIDEMIOLOGICI E PREVENZIONE INFORTUNI	{5}	{4}	{3}	{2}
[DPr.DP] Dati Personali - 196/03	{5}	{4}	{3}	{2}
[DPr.DS] Dati Sensibili e Giudiziari - 196/03	{5}	{5}	{4}	{2}
[DT.LOG] Log	{5}	{5}	{4}	{2}
[DT.DHDK] Dati Help Desk	{4}	{4}	{3}	{2}
[DT.DBCK] Dati Backup	{5}	{5}	{4}	{2}
[DT.DTC] Dati tecnici Ced	{5}	{5}	{4}	{2}
[uff] Uffici	{4}	{3}	{1}	{1}
[LCED] CED	{5}	{4}	{2}	{1}
[EDI] Edificio	{5}	{4}	{2}	{0}

ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO S.I.A. Sistemi Informativi Automatizzati	**ANALISI DEI RISCHI** **PROGETTO ISMS** **EXECUTIVE SUMMARY** **Ambito: SIA** **Data: 14/12/2007** **Rapporto N.: 200701**	Rev. 1 Pag.20 /22 ***Riservato***

Gap UNI-ISO 27001:2005



ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO S.I.A. Sistemi Informativi Automatizzati	**ANALISI DEI RISCHI PROGETTO ISMS** **EXECUTIVE SUMMARY** **Ambito: SIA** **Data: 14/12/2007** **Rapporto N.: 200701**	Rev. 1 Pag.21 /22 ***Riservato***

Confronto media questionario PAC

Sezione	ISPESL Questionario	Ponderata	Media PAC	Contenuti
KPI1	8,25	7,00	7,33	• Modello organizzativo per l'amministrazione dei sistemi, definizione di policy, controllo degli accessi alle risorse e certificazioni richieste. • Sistemi per l'autenticazione. • Aggiornamento S.O. dei server e Software Distribution per le PDL. • Strumenti per il Backup/Restore
KPI2	7,60		7,08	• Sicurezza fisica • Sicurezza perimetrale e controllo accessi ai locali tecnici • Apparati attivi per la sicurezza degli accessi quali firewall, sistemi per la rilevazione delle intrusioni o per la prevenzione • Reti wireless e contromisure per aumentare la sicurezza delle reti wireless • Modalità di accesso da remoto e strumenti utilizzati quali VPN
KPI3	5,50		5,47	• Continuità operativa, procedure da attivare e disponibilità di un piano di disaster recovery • Servizi centralizzati quali antivirus o antispam sulla posta in transito o sulle PDL • Protezione dei contenuti e web filtering. • Capacità di rilevare le intrusioni, e/o prevenirle in funzione del tipo di attacchi già subiti
KPI4	4,75	3,25	5,41	• Ricoprire i ruoli previsti dal DM del 16/02/2002, e tutti i ruoli "noti" nell'ambito della sicurezza • Gestire adeguatamente gli incidenti • Definire policy e curare un budget esplicitamente dedicato alla sicurezza • Gestire adeguatamente le eventuali risorse esterne per la gestione della sicurezza • Avviare iniziative per garantire sviluppi futuri su questi temi

La ponderazione è stata fatta secondo i livelli di maturità del sistema in base alle risultanze dell'analisi EAR/PILAR secondo la seguente logica:

Valore risposta X*Lx (livello)

Dove Lx vale

- 0.10 L1 iniziale / ad hoc
- 0.50 L2 riproducibile ma intuitivo
- 0.90 L3 processo definito
- 0.95 L4 gestito e misurabile
- 1 L5 ottimizzato

Legenda:

Conformità media PAC
Non Conforme
Quasi Conforme
Conforme

Acronimi

- **CERT** – Computer Emergency Response Team
- **CVSS** – Common Vulnerability Scoring System
- **EAR/PILAR** - Entorno de Análisis de Riesgos/Pacchetto Informatico e Logico di Analisi dei Rischi
- **FIRST** – Forum of Incident Response and Security Teams
- **IDS** – Intrusion Detection System
- **IS** - International Standard
- **ISMS** – Information Security Management System
- **ISO** - International Standard Organization
- **KPI** - Key Performance Indicator
- **MAGERIT** – Metodologia di Analisi e GEstione dei Rischi per l'Information Tecnology
- **NIAC** - National Infrastracture Advisory Council
- **UNI** - Ente Nazionale Italiano di Unificazione

fine documento

PROGETTO ISMS

FINALITA' DEL PROGETTO

- Gestione sicura delle informazioni dell'Istituto ai sensi del DLgs 196/2003
- Gestione organica e coordinata dell'infrastruttura informatica dell'Istituto
- Miglioramento Organizzativo sul modello PDCA (Standard UNI/ISO 27001)
- Attività da svolgere a breve ed a medio termine
- Start-up processo certificativo secondo la norma UNI/ISO 27001

L'IMPEGNO DELLA DIREZIONE

ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO
Sistemi Informativi Automatizzati

[illegible] Istituto Superiore per la [illegible] Sicurezza del Lavoro - ISPESL, a norma dell'articolo 9 del decreto legislativo 29 [illegible] 1999 [illegible]

[illegible] 1993, n. 39 [illegible] Norme in [illegible] sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2 [illegible] lettera mm) della legge 23 ottobre 1992, n. 421;

[illegible] legislativo 7 marzo 2005, n. 82

[illegible] legislativo 4 aprile 2006, n. 159 [illegible] integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale;

[illegible] 2002 "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali" del Ministro per l'innovazione e le tecnologie, d'intesa con il Ministro delle comunicazioni

[illegible] pubblica amministrazione digitale"

[illegible] progetto di Risk Analysis, Risk Assessment [illegible] della policy di sicurezza informatica

[illegible] Risk Analysis, Risk Assessment [illegible] sicurezza informatica e per la corretta utilizzazione del software suddetto è necessario il [illegible] Security Officer

[illegible] Information Security Management System [illegible] indirizzo strategico [illegible] sistema di Sicurezza delle informazioni [illegible]

DETERMINA

[illegible] progetto di Risk [illegible] policy di sicurezza informatica

- [illegible] SIA, PROS.R
- [illegible] UF [illegible]
- [illegible] UF [illegible]
- [illegible] UF [illegible]
- [illegible] UF [illegible]
- [illegible] SIA

[illegible] Comitato [illegible] qualsiasi [illegible]

IL DIRETTORE GENERALE
(Dr. Umberto SACERDOTE)

ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO
Sistemi Informativi Automatizzati

[illegible] Regolamento di organizzazione dell'Istituto [illegible] Prevenzione E la Sicurezza del Lavoro - ISPESL, a norma dell'articolo 9 del decreto legislativo 29 ottobre 1999, n. 419;

VISTO il decreto legislativo 12 febbraio 1993, n. 39 [illegible] in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421;

VISTO il Decreto legislativo 7 marzo 2005, n. [illegible]

VISTO il Decreto legislativo 4 aprile 2006, n. 159 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale";

VISTA la Direttiva 16 gennaio 2002 "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali" del Ministro per l'innovazione e le tecnologie, d'intesa con il Ministro delle comunicazioni

VISTA la Direttiva 18 novembre 2005 "Linee guida per la pubblica amministrazione digitale";

[illegible] presente che [illegible] progetto di Risk Analysis, Risk Assessment [illegible] nell'ambito della policy di sicurezza informatica;

Ravvisata l'urgenza e la necessità di ottenere la fornitura di un software per il sistema di gestione della sicurezza delle informazioni in conformità alla vigente normativa

Tenuto conto che [illegible] ad interpellare la Ditta AT4M Srl in merito alla fornitura del software EAR PILAR

Visto l'ordine alla suddetta ditta [illegible] nota [illegible] 14.000.4296 del 17 ottobre 200[illegible]

Tenuto conto che per il corretto andamento dei lavori di Risk Analysis, Risk Assessment [illegible] della policy di sicurezza informatica e per la corretta utilizzazione del software suddetto è necessario il supporto di un Security Officer;

Considerato che l'Ing. Salvatore D'Emilio [illegible] capacità [illegible] incarico

DETERMINA

di nominare l'Ing. Salvatore D'Emilio a Chief Security Officer [illegible] coordinamento nell'ambito del progetto di Risk Analysis, Vulnerability Assessment [illegible] policy di sicurezza informatica. Le mansioni affidate a tale figura sono [illegible] sicurezza del sistema informativo e il supporto alle infrastrutture tecnologiche [illegible] all'esterno, con interazione diretta con il "Comitato di Sicurezza".

IL DIRETTORE GENERALE
(Dr. Umberto SACERDOTE)

PROGETTO ISMS

NOZIONI PRINCIPALI/1

Norma UNI/ISO 27001:

La norma UNI/ISO 27001 introduce il concetto di "Sistema di gestione per la sicurezza delle Informazioni" (SGSI, in inglese ISMS): non è sufficiente implementare una serie di controlli e procedure per la sicurezza informatica , occorre gestirli e mantenerli nel tempo secondo lo schema Plan-Do-Check-Act.

PROGETTO ISMS

NOZIONI PRINCIPALI/2

PDCA :

modello dei sistemi di gestione articolato attraverso le fasi della definizione, realizzazione, esercizio, monitoraggio, revisione, manutenzione e miglioramento continuo dei processi

PROGETTO ISMS

NOZIONI PRINCIPALI/3

SISTEMA INFORMATIVO:

Metodo automatizzato o meno di gestione dei dati aziendali

ASSET:

risorse del sistema informativo o ad esso collegate, necessarie affinchè l'Organizzazione operi correttamente e raggiunga gli obiettivi impostati dalla sua Direzione.

PROGETTO ISMS

NOZIONI PRINCIPALI/4

RISCHIO:

stima del grado di esposizione verso la concretizzazione di una minaccia su di uno o più asset, dannosa per l'Organizzazione

ANALISI DEI RISCHI :

fase di fondamentale importanza nella realizzazione della gestione sicura delle informazioni. Aiuta a delineare la direzione che i futuri provvedimenti sulla sicurezza dovranno essere condotti e da' una buona valutazione per l'acquisizione e l'uso delle contromisure per la sicurezza.

La cieca applicazione di contromisure senza prima aver compreso i rischi a cui può essere soggetto il sistema in esame è quasi sempre poco produttiva, sia da un punto di vista economico che tecnico

PROGETTO ISMS

LEGGI E NORMATIVE DI RIFERIMENTO

- DLgs 30/2005 "Legge sulla tutela del software"
- DLgs 196/2003 "Codice in materia di protezione dei dati personali"
- DLgs 300/1997 "Statuto dei lavoratori"
- Legge 547/1993 "Legge sulla criminalità informatica" e successive modifiche
- Norma UNI/ISO 27001-2007 "Information Security Management System" (2005)
- Quaderno CNIPA N. 28 "Linee guida alla continuità operativa nella Pubblica Amministrazione"
- Quaderno CNIPA N. 23 "Linee guida per la sicurezza ICT nella Pubblica Amministrazione"
- Opuscolo CNIPA N. 10 "La Continuità operativa nella Pubblica Amministrazione"

5.2.1 LA PIANIFICAZIONE DELLA SICUREZZA

In generale, la pianificazione della sicurezza deve considerare lo scenario di rischio ed i vincoli di natura contrattuale e normativa. Questa pianificazione deve essere periodicamente rivista per tenere conto delle variazioni del contesto e per migliorare le protezioni in funzione delle esperienze intercorse.

Ciascuna amministrazione dovrà considerare periodicamente le problematiche di sicurezza che la riguardano e pianificare le azioni necessarie per ottenere una adeguata tutela delle informazioni gestite.
È inoltre opportuno che questa fase di pianificazione sia formalizzata in un documento, condiviso dal vertice dell'organizzazione, all'interno del quale siano riportate le soluzioni che si intende adottare e le relative motivazioni.

Fonte CNIPA Q. 23