ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO
Dipartimento del bilancio, del personale e degli affari generali
Unità Funzionale V

C. Analisi dei rischi. Tabella 3.

Si riporta la tabella aggiornata in merito all'analisi dei rischi ed all'individuazione ed adozione delle relative misure di protezione e di sicurezza relativa al Dipartimento Medicina del Lavoro.

Tabella 3 - ANALISI DEI RISCHI (DML)

Rischi	Si / No	Descrizione dell'impatto sulla sicurezza (gravità alta media bassa)
Sottrazione di credenziali di autenticazione	NO	
Carenza di consapevolezza, disattenzione o incuria	NO	
Comportamenti sleali o fraudolenti	NO	
Errore materiale	SI	BASSA
Azione di *virus* informatici o di programmi	SI	BASSA
Spamming o tecniche di sabotaggio	NO	
Malfunzionamento, indisponibilità o degrado degli strumenti	SI	BASSA
Accessi esterni non autorizzati	NO	
Intercettazione di informazione in rete	SI	BASSA
Accessi non autorizzati a locali/reparti ad accesso ristretto	NO	
Sottrazione di strumenti contenenti dati	NO	
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali,...) nonché dolosi, accidentali o dovuti ad incuria	SI	BASSA
Guasto ai sistemi complementari (impianto elettrico, climatizzazione,...)	NO	
Errori umani nella gestione della sicurezza fisica	SI	BASSA
Altro evento	NO	

Comportamenti degli operatori

ISTITUTO SUPERIORE PER LA PREVENZIONE E LA SICUREZZA DEL LAVORO
Dipartimento del bilancio, del personale e degli affari generali
Unità Funzionale V

D) Attività del Servizio Sistemi informativi automatizzati:

- **Documento di analisi dei rischi,** volto alla protezione delle informazioni gestiti mediante l'infrastruttura di rete dell'Istituto;
- **Progetto ISMS,** volto alla certificazione del CED secondo la norma ISO/IEC 27001.

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.1 /22 ***Riservato***

Progetto ISMS - Analisi dei rischi

Documento di Sintesi

CODICE: DS01
VERSIONE: 1.0

Codice	**DS01**		
Classificazione	**RISERVATO**		
Autorizzati	**Comitato di Sicurezza**		
Autore	**D'Emilio/Merlo**		
Nome file	**Executive Summary**		
Versione	**1.0**	Stato	**Approvato**
Approvato da			
Data creazione	**14/12/2007**	Data ultimo aggiornamento	

Si rammentano le seguenti Note Operative:
1. I documenti classificati "ad uso interno" non possono essere divulgati all'esterno dell'ISPESL.
2. La persona che venisse in possesso di un documento classificato "riservato" e non trovi il suo nominativo nella lista del personale autorizzato al suo utilizzo è invitato a consegnare il documento ad una delle persone citate nella lista di cui sopra.

CRONOLOGIA

Data	Autore	motivazione
14/12/2007	D'Emilio/Merlo	Release 1.0

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.3 /22 ***Riservato***

INDICE

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.4 /22 ***Riservato***

Finalità

Scopo del documento è presentare, sinteticamente, le risultanze dell'analisi dei rischi eseguita nell'ambito delle attività di Risk Analisys e Risk Assessment.
La documentazione completa dell'attività svolta, dalla quale si sono desunte le conclusioni esposte è reperibile nell'area del sito dedicata al Comitato Sicurezza.

Considerazioni di sintesi

L'analisi, condotta secondo diverse metodologie, in dipendenza dell'area da esaminare (tecnica o gestionale/organizzativa), ha portato ad individuare alcune criticità da sottoporre ad azioni correttive, ipotizzate realizzabili almeno parzialmente, entro il 2009.
Nell'area tecnica il problema principale nasce dalla mancanza di un sistema IDS (Intrusion Detection System), mentre l'architettura adottata è conforme alle best practice esistenti.
Un numero limitato di vulnerabilità di livello alto sono state riscontrate nelle configurazione delle macchine e sono già state inviate al Security Forum per gli adempimenti di competenza.
Un discorso a parte merita l'analisi approfondita delle vulnerabilità legate alla continuità operativa ed, eventualmente, al disaster recovery, che dovrà essere affrontata in un apposito studio nell'ambito del progetto, entro il 2008.
Le maggiori criticità si sono individuate, come atteso in un sistema in fase di start up, nell'area gestionale organizzativa.
In quest'area le difficoltà maggiori sono dovute a due fattori:

1. necessità di coinvolgere, almeno parzialmente, tutto il personale dell'ambito in esame;
2. mancanza di strumenti standardizzati (metriche), a livello nazionale od internazionale, per misurare l'efficacia delle contromisure adottate.

Sul coinvolgimento del personale, totale per quanto riguarda corsi di formazione di base sulla sicurezza delle informazioni, è necessario un forte impegno della Direzione; la seconda criticità porta a chiedere al C.S. di approvare, per i rischi residui legati ai dati sensibili, l'innalzamento dal livello 1 (basso) a livello 2 (medio basso), in attesa che esca uno standard nazionale in materia di metrica o che l'ISO emani il documento 27004, in fase di studio. L'alternativa a questa soluzione richiede l'adozione di metriche esistenti, ma non standard riconosciuti a livello nazionale o internazionale, con la necessità di dover successivamente adottare metodologie diverse e riconvertire tutto il lavoro svolto, o la creazione di un proprio sistema. In ambedue i casi non si ritiene che il rapporto costo/benefici giustifichi l'impegno necessario.
Allo stato dell'arte si può ipotizzare che la deroga alla policy sia necessaria per tutto il 2009.
In relazione alla possibile certificazione UNI-ISO IS 27001:2005 le attività individuate, se adottate, consentono di portare il sistema da un livello di conformità del 10% (situazione attuale) ad un livello del 90% entro il 2009, quindi certificabile con un minimo sforzo

aggiuntivo.
La verifica effettuata, inoltre, con il questionario CNIPA per valutare il livello di sicurezza delle PAC, confrontando i livelli raggiunti dall'ISPESL con la media PAC, conferma che le aree di miglioramento sono quelle individuate dalle analisi interne effettuate

Metodologia.

I rischi sono stati esaminati secondo due aspetti, quello tecnologico e quello organizzativo.
Per l'aspetto tecnologico si è analizzata l'architettura del sistema in esame, per verificarne la rispondenza alle esigenze di sicurezza poste, e si è effettuato un test per determinarne il livello di rischio secondo la metodologia di valutazione CVSS (Common Vulnerability Scoring System).
Il Cvss è nato su iniziativa del Niac (National Infrastructure Advisory Council) statunitense e divulgato dal Department of Homeland Security (di cui il Niac fa parte). La garanzia dell'imparzialità e della correttezza della metodologia stessa è demandata al First (Forum of Incident Response and Security Teams).
L'analisi vera e propria è stata eseguita effettuando un probe tramite il tool Nessus, quindi verificando sul sistema reale le eventuali debolezze.
Il probe è stato effettuato operando sia sulla rete interna, sia sulla rete pubblica, per simulare attacchi provenienti da ambienti diversi.
Per l'aspetto gestionale/organizzativo si è utilizzata la metodologia MAGERIT (Metodologia di Analisi e GEstione dei Rischi per l'Information Technology), sviluppata in Spagna a partire dal Centro Nazionale di Intelligence e il Centro Crittografico Nazionale per il Ministero della Pubblica Amministrazione. Tale metodologia è orientata a mettere in risalto, pur non trascurando aspetti tecnici, la rilevanza degli aspetti gestionali nell'attuazione di un ISMS.
L'analisi è stata eseguita utilizzando il tool EAR/PILAR, disponibile anche in italiano, acquisendo le informazioni sullo stato dell'arte tramite audit condotti dal CSO.
Sono state prese in esame le minacce che attentino alla disponibilità, integrità e riservatezza delle informazioni.
Per rendere i risultati delle due metodologie confrontabili, si è provveduto ad uniformare i livelli di rischio ottenuti (forniti su scale diverse) come segue:

Livello CVSS	Livello MAGERIT	Tipologia
8, 9, 10	*5*	***Rischio elevato***
6, 7	*4*	***Rischio medio alto***
4, 5	*3*	***Rischio medio basso***
2, 3	*2*	***Rischio basso medio***
1	*1*	***Rischio basso***

Si è utilizzato, infine, il questionario predisposto dal CNIPA per raccogliere i dati necessari alla stesura dell'annuale rapporto sulla sicurezza delle PAC, in modo da avere un benchmark significativo per il settore. In questo ultimo caso si è provveduto, inoltre, a pesare i risultati ottenuti integrandoli con le evidenze emerse dalle altre analisi, al fine di

integrare le semplificazioni del questionario stesso.
Il questionario consta di 36 quesiti e 13 sottoquesiti a risposta chiusa, raccolti in sottosezioni ed associati ai seguenti KPI (Key Performance Indicator);

- KPI1: Sicurezza logica
- KPI2: Sicurezza dell'infrastruttura
- KPI3: Sicurezza dei servizi
- KPI4: Sicurezza dell'organizzazione

La valutazione dei risultati va letta in base alla seguente scala:

0≤KPI<4	**scarsa**	**Valori critici che nella media stabiliscono un sostanziale disinteresse rispetto al tema Sicurezza**
4≤KPI<5	**accettabile**	**Valori mediocri per molti quesiti è possibile con sforzi non rilevanti ottenere buoni margini di miglioramento.**
5≤ KP<7	**buona**	**Valori positivi che con interventi mirati sono passibili di ulteriori miglioramenti**
7≤KPI≤10	**ottima**	**Valori medi accettabili per gli attuali requisiti in termini di sicurezza per i quesiti che compongono il KPI.**

I risultati delle analisi del probe sono stati indirizzati al Security Forum che li ha presi in carico e provvederà, a breve, a fornire ipotesi di soluzione.
I risultati dell'analisi EAR/PILAR sono stati utilizzati per ipotizzare due scenari (a breve – 2008 ed a medio – 2009) di evoluzione gestionale/organizzativa al fine di mitigare i rischi, in ottica dell'adozione di in ISMS conforme allo standard UNI-ISO IS 27001:2005.

Risultanze delle analisi.

Le risultanze delle analisi sono state suddivise in base alle aree ed agli scenari temporali ipotizzati (attuale, a breve – 2008, a medio – 2009). Nell'individuazione e proposta delle attività da svolgere si è tenuto conto delle risorse umane disponibili e delle altre attività aziendali. Va ricordato che un ISMS è un processo continuo, pertanto almeno una volta all'anno va effettuata una sua revisione, con l'aggiornamento delle analisi dei rischi effettuate e la eventuale adozione delle misure necessarie a mantenerlo efficiente.

Situazione attuale

Area tecnologica

Architettura
L'esame dell'architettura ha rilevato che il sistema è fondamentalmente conforme alle best practice in vigore, con l'unica eccezione della mancanza di un IDS.

CVSS
Le risultanze di Nessus hanno fornito i seguenti risultati:

- Nessuna vulnerabilità rilevata per eventuali attacchi da rete pubblica;
- Vulnerabilità di livello alto (in numero limitato) per eventuali attacchi da rete interna.

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.7 /22 ***Riservato***

Area gestionale/organizzativa

Le risultanze di EAR/PILAR per l'area gestionale/organizzativa hanno evidenziato, come era da attendersi per un sistema in start-up, numerose aree di rischio elevato.

Situazione a breve

Architettura

Studio di fattibilità relativo all'installazione di un IDS.
Il lavoro deve essere eseguito con la corretta ed attenta individuazione delle difficoltà possibili nella corretta configurazione del prodotto, per evitare che falsi positivi e negativi ed eccessiva difficoltà nella gestione degli allarmi ne inficino l'adozione.

CVSS

- Risoluzione delle criticità a livello alto e medio riscontrate;
- esame delle criticità a livello basso per valutare la convenienza della loro risoluzione
- esecuzione di probe trimestrali di verifica, due almeno dei quali fatti eseguire da società esterne, per avere più risultati

Area gestionale/organizzativa

Le attività nell'area gestionale/organizzativa sono quelle che richiedono un maggior impegno per raggiungere gli obiettivi previsti.

A breve si ipotizza:

- stesura delle principali policy necessarie e revisione delle esistenti;
- formazione del personale, non solo tecnico, sulla sicurezza delle informazioni;
- istituzione di un CERT (Computer Emergency Response Team) per la gestione degli incidenti;
- analisi degli impatti legati a minacce riguardanti la continuità operativa e relativo progetto;
- partecipazione ad attività significative (esterne all'Istituto) sulla sicurezza;
- revisione dell'ISMS

Situazione a medio

Architettura

Eventuale installazione dell'IDS.
Eventuale aggiornamento del sistema per consentire la gestione della continuità operativa.

CVSS

- esecuzione di probe trimestrali di verifica,due almeno dei quali fatti eseguire da società esterne, per avere più risultati;
- risoluzione delle criticità a livello alto e medio eventualmente riscontrate;
- esame delle eventuali criticità a livello basso per valutare la convenienza della loro risoluzione

Area gestionale/organizzativa

- stesura delle norme tecniche e complementari necessarie e revisione delle esistenti;
- formazione del personale, non solo tecnico, sulla sicurezza delle informazioni;
- partecipazione ad attività significative (esterne all'Istituto) sulla sicurezza;
- revisione dell'ISMS

ALLEGATI

Si riportano negli allegati le risultanze sintetiche delle varie analisi (Nessus, EAR/PILAR e CNIPA). I documenti originali sono reperibili nella apposita cartella condivisa, riservata al Comitato di Sicurezza.
La scala cromatica utilizzata rispetta i seguenti valori:

Valori di Rischio
Rischio elevato
Rischio medio alto
Rischio medio basso
Rischio basso medio
Rischio basso

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.10 /22 ***Riservato***

Risultanze Nessus

Server	*Low*	*Medium*	*High*
Server Management	*115*	*11*	*3*
Backup	*94*	*10*	*1*
Oracle	*65*	*5*	*1*
SWTHP	*24*	*3*	*1*
Back End	*38*	*2*	*0*
Front End	*51*	*12*	*0*
Fortigate 2	*17*	*1*	*0*
Domain Controller	*50*	*6*	*0*
Cluster	*39*	*2*	*0*
Svrweb	*12*	*0*	*0*
Proxy	*12*	*1*	*0*
Server RAS	*26*	*1*	*0*
SA-DNS	*21*	*2*	*0*
Terminal Server	*49*	*1*	*0*
Server Sviluppo	*80*	*14*	*0*
Docdw01	*53*	*8*	*0*
Server Protocollo	*44*	*4*	*0*
VSR-VSG	*15*	*1*	*0*
Server Infortuni Mortali	*29*	*5*	*0*
Totale	*834*	*39*	*8*

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.11 /22 ***Riservato***

Risultanze EAR/PILAR

Situazione attuale

asset	[D]	[I]	[R]
[PDL2.PDLA] Posto di lavoro Amministrativi	[4]		
[PDL2.PDLT] Posto di Lavoro Tecnici	[4]		
[AUFF] Sever di Piano per File sharing - 1,7 piani	[5]		
[Area SAS] 2 Server SAS del DPO	[5]		
[CED.DMZ.DMZ RAS] Server RAS - Remote Access Server	[3]		
[CED.DMZ.DMZ Net] Server Proxy (ISA)/Server DNS	[5]		
[CED.DMZ.DMZ WEB] Server Web/Inf Mortali (DPO)/VSR-VSG (DCC)	[5]		
[CED.DMZ.DMZ Apparati di rete] Switch / Firewall	[5]		
[CED.LN.CLEX] CLUSTER EXCHANGE 2fe+2be+1SAN	[5]		
[CED.LN.CL2.SNET] Server di Rete DHCP/File Sharing/Print Sharing	[5]		
[CED.LN.CL2.SQL] SQL 2005	[5]		
[CED.LN.SAN] Storage Area Network	[5]		
[CED.LN.SRV DC] 2 SERVER DI DOMAIN CONTROLLER+WSUS	[5]		
[CED.LN.TS] TERMINAL SERVER	[4]		
[CED.LN.BCK] SERVER BACKUP	[4]		
[CED.LN.ORL] SERVER ORACLE per DML	[4]		
[CED.LN.MNG] SERVER ANTIVIRUS ED HELP DESK	[5]		
[CED.LN.SW] SERVER DI SVILUPPO WEB	[3]		
[WAN] Switch WAN/VPN Concentrator	[4]		
[LAN] LAN Via Alessandria	[5]		
[UCED.AS] AMMINISTRATORI SISTEMA	[5]		
[UCED.OShd] OPERATORE HELP DESK	[4]		
[UCED.EXT] PERSONALE ESTERNO	[5]		
[PEXT2.EXT2] Personale esterno al CED	[3]		
[UA.PU] PERSONALE AMMINISTRATIVO UTENTE	[4]		
[Appl] Software applicativo - installato di base sui pc	[5]		
[Base.BKP] ARCSERVE BRIGTSTORE BACKUP	[4]		
[Base.ORC] Oracle	[4]		
[Base.DB] SQL 2005	[5]		
[COWIN.Sow] Windows server 2003	[5]		
[COWIN.SOW2] Sistema Operativo WINXP	[5]		

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.12 /22 ***Riservato***

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

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.13 /22 ***Riservato***

Situazione a breve

Asset	[D]	[I]	[R]
[PDL2.PDLA] Posto di lavoro Amministrativi	(2)		
[PDL2.PDLT] Posto di Lavoro Tecnici	(2)		
[AUFF] Sever di Piano per File sharing - 1.7 piani	(3)		
[Area SAS] 2 Server SAS del DPO	(3)		
[CED.DMZ.DMZ RAS] Server RAS - Remote Access Server	(2)		
[CED.DMZ.DMZ Net] Server Proxy (ISA)/Server DNS	(3)		
[CED.DMZ.DMZ WEB] Server Web/Inf Mortali (DPO)/VSR-VSG (DCC)	(3)		
[CED.DMZ.DMZ Apparati di rete] Switch / Firewall	(3)		
[CED.LN.CLEX] CLUSTER EXCHANGE 2fe+2be+1SAN	(3)		
[CED.LN.CL2.SNET] Server di Rete DHCP/File Sharing/Print Sharing	(3)		
[CED.LN.CL2.SQL] SQL 2005	(3)		
[CED.LN.SAN] Storage Area Network	(3)		
[CED.LN.SRV DC] 2 SERVER DI DOMAIN CONTROLLER+WSUS	(3)		
[CED.LN.TS] TERMINAL SERVER	(2)		
[CED.LN.BCK] SERVER BACKUP	(2)		
[CED.LN.ORL] SERVER ORACLE per DML	(2)		
[CED.LN.MNG] SERVER ANTIVIRUS ED HELP DESK	(3)		
[CED.LN.SW] SERVER DI SVILUPPO WEB	(2)		
[WAN] Switch WAN/VPN Concentrator	(2)		
[LAN] LAN Via Alessandria	(3)		
[UCED.AS] AMMINISTRATORI SISTEMA	(4)		
[UCED.OShd] OPERATORE HELP DESK	(3)		
[UCED.EXT] PERSONALE ESTERNO	(4)		
[PEXT2.EXT2] Personale esterno al CED	(1)		
[UA.PU] PERSONALE AMMINISTRATIVO UTENTE	(3)		
[Appl] Software applicativo - installato di base sui pc	(4)		
[Base.BKP] ARCSERVE BRIGTSTORE BACKUP	(3)		
[Base.ORC] Oracle	(3)		
[Base.DB] SQL 2005	(4)		
[OWIN.Sow] Windows server 2003	(5)		