PROGETTO ISMS

COMITATO DI SICUREZZA

Organismo interno rappresentante tutte le funzioni che partecipano alla gestione dell'ISMS.

OBIETTIVI DEL COMITATO:

- **Fornire indirizzo strategico al Forum di Sicurezza in materia di Sicurezza delle Informazioni, incentivare e seguire le iniziative in materia**
- **Esaminare ed approvare le Politiche ad alto livello**
- **Esaminare la risoluzione degli incidenti di Sicurezza delle Informazioni**
- **Approvare le principali iniziative per migliorare la Sicurezza delle Informazioni**

Si riunisce di regola con cadenza trimestrale ed in via straordinaria con richiesta di un membro

PROGETTO ISMS

FORUM DI SICUREZZA

Organismo interno maggiormente orientato alle tematiche tecniche ed operative, con il mandato di controllare lo stato di funzionamento e di implementazione dell'Information Security Management System e di preparare rapporti da sottoporre al Comitato

OBIETTIVI DEL FORUM:

- **Eseguire Audit ISMS**
- **Correzioni "tecniche" alle situazioni di non conformità riscontrate**
- **Sottoporre al Comitato le azioni non tecniche**
- **Gestione degli incidenti**

Il CSO, coordinatore del Forum, funge da segretario del Comitato

PROGETTO ISMS

STATO DELL'ARTE

- **ANALISI PRELIMINARE DEL SISTEMA INFORMATIVO:**

definizione e pianificazione dell'ambito del progetto, censimento e valorizzazione di tutti gli asset, caratterizzazione delle minacce e delle contromisure, valutazione dello stato di rischio (analisi qualitativa)

- **Redazione prime policy di sicurezza**

PROGETTO ISMS

TEMPIFICAZIONE/1

Numero	Attività	Durata	Inizio	Fine	Predecessori
1	AGR - Analisi e gestione dei rischi (qualitativa)	44g	mer 17/10/07	lun 17/12/07	
2	*Attività preliminari*	4g	mer 17/10/07	lun 22/10/07	
3	Definizione perimetro	1g	mer 17/10/07	mer 17/10/07	
4	Pianificazione progetto	3g	gio 18/10/07	lun 22/10/07	3
5	*D - Progetto*	1g	mar 23/10/07	mar 23/10/07	4
6	definizione parametri EAR	1g	mar 23/10/07	mar 23/10/07	4
7	incontro di verifica	1g	mar 23/10/07	mar 23/10/07	6
8	incontro con consulente	1g	mar 23/10/07	mar 23/10/07	6
9	*A - Analisi dei rischi*	23g	mer 24/10/07	ven 23/11/07	
10	*A1-asset*	12g	mer 24/10/07	gio 08/11/07	
11	inserimento asset	4g	mer 24/10/07	lun 29/10/07	5
12	dipendenza tra asset	3g	mar 30/10/07	gio 01/11/07	11
13	Definizione politica generale	4g	lun 29/10/07	gio 01/11/07	
14	valorizzazione asset	5g	ven 02/11/07	gio 08/11/07	13
15	*A2 - minacce*	7g	ven 09/11/07	lun 19/11/07	
16	identificazione minacce	1g	ven 09/11/07	ven 09/11/07	14
17	valorizzazione minacce	6g	lun 12/11/07	lun 19/11/07	16

PROGETTO ISMS

TEMPIFICAZIONE/2

18	*A3 - Impatto e rischio*	*3g*	*ven 30/11/07*	*ven30/11/07*	
19	impatto/rischio/tabella	3g	ven 30/11/07	ven 14/12/07	17
20	**Primo incontro Comitato**	**1g**	**gio 29/11/07**	**gio 29/11/07**	
21	*T - Trattamento dei rischi*	*15g*	*lun 30/11/07*	*ven 14/12/07*	
22	*T.0. Fasi del progetto*	*1g*	*lun 30/11/07*	*ven 14/12/07*	*21*
23	*T.P. Politica di sicurezza*	*10g*	*mar 27/11/07*	*ven14/12/07*	*23*
24	Formalizzazione Politica generale	1g	gio 29/11/07	gio 29/11/07	
25	Formalizzazione Procedure di sicurezza	9g	ven 30/11/07	gio 14/12/07	25
26	*T.1. Contromisure*	*2g*	*ven30/11/07*	*ven 14/12/07*	*"26,23"*
27	*T.3. Impatto e rischio residui*	*2g*	*gio 30/11/07*	*ven 14/12/07*	*27*
28	incontro di verifica con consulente	1g	gio13/12/07	gio 13/12/07	
29	incontro di verifica con Comitato	1g	ven 14/12/07	ven14/12/07	28

PROGETTO ISMS

POLITICA DI SICUREZZA ISPESL

CLASSIFICAZIONE DEI DATI

PUBBLICI – dati che sono di pubblico dominio

AD USO INTERNO – dati non critici ma di pertinenza del solo Istituto

RISERVATI – dati di particolare interesse e criticità per l'attività dell'Istituto e/o definiti tali dalle leggi vigenti

SENSIBILI - definiti tali dalle leggi vigenti

REQUISITI DI SICUREZZA:

PUBBLICI – disponibilità, integrità

AD USO INTERNO – disponibilità, integrità, riservatezza

RISERVATI –disponibilità, integrità, riservatezza

SENSIBILI - disponibilità, integrità, riservatezza

PROGETTO ISMS

CLASSIFICAZIONE DEI LIVELLI DI RISCHIO

Livello	Tipologia	Note
5	**Rischio elevato**	**Non accettabile**
4	**Rischio medio alto**	**Accettabile per un tempo limitato per dati non critici**
3	**Rischio medio basso**	**Accettabile per dati non critici**
2	**Rischio basso medio**	**Accettabile per dati a criticità media**
1	**Rischio basso**	**Per dati ad alta criticità**

PROGETTO ISMS

RISCHIO RESIDUO ACCETTATO PER TIPOLOGIA DI DATO

Tipologia	Dimensioni	A breve (2008)	A medio (2009)
pubblici	disponibilità, integrità	4 4	3 3
ad uso interno	disponibilità, integrità, riservatezza	4 4 4	3 3 3
riservati	disponibilità, integrità, riservatezza	3 3 3	2 2 2
sensibili	disponibilità, integrità, riservatezza	2 2 2	1 1 1

PROGETTO ISMS

PRIMA ANALISI/1

TIPOLOGIA	CLASSIFICAZIONE	RISCHIO ACCETTABILE A BREVE	RISCHIO ACCETTABILE A MEDIO
DATI PRIVACY - 196/03			
Dati Personali - 196/03	RISERVATI	3	2
Dati Sensibili - 196/03	SENSIBILI	2	1
DATI TECNICI			
Log	RISERVATI	3	2
Dati Help Desk	USO INTERNO	4	3
Dati Backup - anche configurazioni macchine server	RISERVATI	3	2
Dati tecnici Ced	RISERVATI	3	2

PROGETTO ISMS

PRIMA ANALISI/2

DATI COMMERCIALI	CLASSIFICAZIONE	RISCHIO ACCETTABILE A BREVE	RISCHIO ACCETTABILE A MEDIO
contabilità di bilancio	RISERVATI	3	2
Contratti di lavoro dipendenti	RISERVATI	3	2
Contratti Fornitori	RISERVATI	3	2
Contratti Clienti	RISERVATI	3	2
DATI TIPICI ISPESL			
Dati Ricerca - Documentazione tecnica - Statistiche	PUBBLICI	4	3
Dati Omologazione e Certificazione	AD USO INTERNO	4	3
Dati Sicurezza sul Lavoro – EPIDEMIOLOGICI E PREVENZIONE INFORTUNI	SENSIBILI	2	1

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

E. Misure adottate per prevenire o contrastare i rischi individuati e per garantire l'integrità e la disponibilità dei dati stessi, descritte in forma sintetica nella Tabella 4.1

Si riportano le tabelle aggiornate in merito al Dipartimento Medicina Del Lavoro ed al Dipartimento Territoriale di Verona.

DIPARTIMENTO CENTRALE MEDICINA DEL LAVORO
Tabella 4.1 - LE MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare	Struttura o persone addette all'adozione
a) Antivirus; b) Duplicazione di archivi su supporti elettronici di salvataggio floppy disk CD-ROM; c) Installazione password sistem; d) Installazione password di accesso e data base; e) Tecniche di cifratura a codici identificativi	Perdita dei dati presenti negli archivi; Accesso permesso al solo personale autorizzato al trattamento dei dati.	Gestione dei registri di esposizione e di patologie, delle cartelle sanitarie di rischio e dei DoSP. Attività di ricerca scientifica finalizzata alla tutela della salute e sicurezza dei lavoratori ed alla prevenzione degli infortuni negli ambienti di vita	a) Antivirus; b) Duplicazione di archivi su supporti elettronici di salvataggio floppy disk CD-ROM; c) Installazione password sistem; d) Installazione password di accesso e data base; e) Tecniche di cifratura a codici identificativi		Personale nominato da Direttore Dipartimento

DIPARTIMENTO TERRITORIALE VERONA

Tabella 4.1 LE MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare	Struttura o persone addette all'adozione
a) Antivirus anti spy anti spam		Dipar. Terr. da 1) a 9)	Dalla lett. a) alla j)		SIDPI - SIA Dipendenti del Dipartimento
b) Duplicazione di archivi su supporti elettronici di salvataggio floppy disk CD e disco ottico;					
c) Installazione password sistemi;					SIDPI -
d) Installazione password per singoli file;					
e) Installazione password di accesso server;					
f) Disattivazione credenziali di autenticazione non utilizzate da almeno sei mesi;					
g) Sistema di aggiornamento giornaliero dei software;					

DIPARTIMENTO TERRITORIALE VERONA

Tabella 4.1 - LE MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare	Struttura o persone addette all'adozione
h) Creazione e gestione di diversi profili utente con potere di accesso e modifica dati differenziati in base alle diverse mansioni;					SIDPI - SIA
i) Sistema di back up mediante ripristino della disponibilità dei dati e dei sistemi ogni tre ore;					
j) Firewall;					
k) Il computer del Direttore può collegarsi alla rete SIDPI o a rete esterna solo in alternativa;					SIDPI
m) Un solo apposito computer è dedicato al traffico Internet ed alla posta elettronica e non è connesso alla rete locale dei computer dei singoli					Dipendenti del Dipartimento

DIPARTIMENTO TERRITORIALE VERONA

Tabella 4.1 – LE MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare	Struttura o persone addette all'adozione
dipendenti. Il computer è configurato con password diversa per ogni dipendente.					SIA

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

G. Previsione degli interventi formativi dei responsabili e degli incaricati al trattamento, per renderli edotti dei rischi al momento dell'ingresso in servizio, in caso di cambiamento di mansioni o di introduzione di nuovi strumenti informatici, per il trattamento dei dati.

È proseguita l'attività di formazione ed informazione in ordine agli aspetti sostanziali e formali del TU sulla Privacy – D. Lgs. 196/2003, con un corso in aula organizzato per i giorni 11 e 12 ottobre 2008 nella Sede Centrale per gli incaricati del trattamento dei dati sensibili e giudiziari, già previsto con circolare n. 2/2008 np. AOO15/0000381 del 6/2/2008.

Un ulteriore corso per gli incaricati del trattamento dei dati sensibili e giudiziari è in corso di programmazione al fine di completare la formazione di tutto il personale incaricato del trattamento dei suddetti dati, così come per i responsabili del trattamento.

E' stato, altresì, programmato un corso multimediale interattivo per formare ed informare tutto il personale incaricato dei trattamenti di dati personali.