

000006



# AZIENDA SANITARIA LOCALE - A.S.L. DELLA PROVINCIA DI VARESE

D.P.G.R. N. 70640 DEL 22.12.1997

**Verbale delle deliberazioni dell'anno 2009****DELIBERAZIONE DEL DIRETTORE GENERALE****- 9 GEN. 2009**  
INDATA 2009 N. 2

OGGETTO: D.Lgs 196/2003 "Codice in materia di protezione dei dati personali" – Consulenza per la revisione dell'Analisi dei Rischi degli archivi contenenti dati sensibili e/o giudiziari finalizzata all'aggiornamento del Documento Programmatico (DPS) aggiornamento marzo 2008/2009 dell'ASL della Provincia di Varese.

## IL DIRETTORE GENERALE

nella persona del Dr. Pierluigi Zeli

ASSISTITO DA:

IL DIRETTORE AMMINISTRATIVO

DR. MASSIMO LA VESSI

IL DIRETTORE SANITARIO

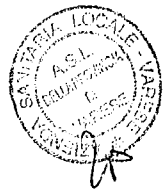
DR. ELIO GIORGIO MARMONDI

000007



- Premesso che con deliberazione n. 239 del 9 marzo 2005 sono stati approvati il “Documento Programmatico sulla Sicurezza” e il “Regolamento sull’utilizzo delle risorse informatiche aziendali” mediante il supporto della consulenza stipulata nell’anno 2004 – a seguito di procedura negoziata – con la ditta GFI OIS spa di Roma finalizzata all’attuazione della normativa di cui al D.Lgs 196/2003;
- Premesso altresì che con successivi provvedimenti deliberativi la predetta Società veniva incaricata per l’erogazione di attività finalizzata al continuo aggiornamento dell’Analisi dei Rischi degli archivi/banche dati informatici aziendali contenenti dati sensibili e/o giudiziari e dell’adeguamento del Documento Programmatico (DPS) per quanto riguarda la verifica sullo stato di sicurezza del sistema informativo/informatico;
- Considerato che la materia di che trattasi è soggetta a frequenti innovazioni in ambito giuridico e organizzativo e che inoltre la vigente normativa in materia obbliga al continuo aggiornamento ed adeguamento del Documento Programmatico attraverso il riesame delle eventuali vulnerabilità del sistema informativo/informatico alla luce dei cambiamenti tecnologici intervenuti;
- Vista l’allegata relazione prot. n. 2008/014SI0014665/I del 26/11/2008 con la quale il Dirigente Ingegnere – Responsabile del CED, nelle more di espletamento delle procedure di gara per rinnovare la consulenza informatica e per garantire la continua e regolare attuazione del Decreto Legislativo 196/2003, propone alla Direzione Aziendale l’affidamento alla Società GFI Italia delle attività finalizzate al raggiungimento di tre precisi obiettivi, inviando contestualmente l’offerta tecnica ed economica prot. n. 2008/014P0109113 del 7/11/2008:
  1. Realizzazione dell’ “Allegato A – Analisi dei Rischi” da allegare al DPS aggiornato al 31/03/2008 approvato con provvedimento deliberativo n. 211/2008
  2. Realizzazione di n. 2 procedure parte integrante del DPS aggiornato al 31/03/2009 e precisamente:
    - a. Procedura della gestione degli Account automatica e centralizzata presso il CED
    - b. Procedura di analisi sistemistica dei log e di controllo degli accessi presso il CED
  3. Realizzazione dell’ “Allegato A – Analisi dei Rischi” da allegare al DPS aggiornato al 31/03/2009;
- Rilevato che in merito all’affidamento della consulenza alla società in questione, nelle more di espletamento delle procedure di gara, il Dirigente Ingegnere del CED, nella nota soprarichiamata ed allegata in copia quale parte integrante e sostanziale del presente provvedimento, esprime parere favorevole per i seguenti motivi:
  - *“continuità del servizio già erogato a partire dall’affidamento originale della consulenza avvenuto nell’anno 2004, nelle modalità tecniche ed organizzative (utilizzo della metodologia CRAMM) già adottate dal personale dell’impresa GFI nelle precedenti analisi dei rischi e relativa identificazione delle misure di sicurezza da realizzare per la loro eliminazione*

000008



- sostanziale soddisfazione per quanto finora realizzato con la collaborazione del personale dell'ASL competente in materia
  - congruità dell'offerta economica nel rapporto costi/benefici, pari ad € 12.000,00 oltre IVA, ritenuta corrispondente all'impegno previsto e allineata alle tariffe di mercato";
- Vista la nota del 23/12/2008 prot. n. 2008/014SI0016070/I ad oggetto "Richiesta di espletamento delle procedure di gara per rinnovare la Consulenza informatica per l'anno 2009 per l'attuazione del Decreto Legislativo 196/2003 riguardante il Codice in materia di Protezione dei Dati Personali" con la quale il Responsabile del Servizio Affari Generali e Legali e il Dirigente Ingegnere – Responsabile CED trasmettono al Responsabile del Servizio Gestione Approvvigionamenti l'Allegato Tecnico al capitolato per l'affidamento del servizio di consulenza e assistenza nell'attuazione del codice in materia di protezione dei dati personali;
- Preso atto delle motivazioni addotte a sostegno della proposta e ritenuto di aderirvi, tenuto conto anche che la continuità tecnico-organizzativa ad oggi realizzata ha permesso di conseguire risultati soddisfacenti;
- Esaminata l'allegata offerta pervenuta da GFI Italia SpA in data 7/11/2008 prot. ASL n. 2008/014P0109113 e ritenuto di approvarne i termini e le condizioni, atteso altresì il parere favorevole e la congruità dei costi espressi da Responsabile del CED nella richiamata relazione;
- Visto il vigente Regolamento per l'acquisto di beni e servizi in economia ai sensi e per gli effetti dell'art. 125 del Decreto Legislativo 12.04.2006, approvato con provvedimento del Direttore Generale n. 489 del 13 agosto 2008;
- Ritenuto per quanto sopra di provvedere al conferimento della consulenza di che trattasi per il conseguimento degli obiettivi descritti nei precedenti capoversi e con le modalità, i termini e le condizioni di cui alla relazione e all'offerta citata;
- Acquisiti i pareri favorevoli dei Direttori Sanitario ed Amministrativo, con ricezione del presente provvedimento a cura di quest'ultimo;

DELIBERA

Per le ragioni di cui in parte motiva:

1. di conferire alla società GFI Italia SpA con sede in Roma – incarico di consulenza per le attività finalizzate al raggiungimento di tre precisi obiettivi:
  - Realizzazione dell' "Allegato A – Analisi dei Rischi" da allegare al DPS aggiornato al 31/03/2008 approvato con provvedimento deliberativo n. 211/2008
  - Realizzazione di n. 2 procedure parte integrante del DPS aggiornato al 31/03/2009 e precisamente:

000009



- Procedura della gestione degli Account automatica e centralizzata presso il CED
  - Procedura di analisi sistemistica dei log e di controllo degli accessi presso il CED
  - Realizzazione dell' "Allegato A - Analisi dei Rischi" da allegare al DPS aggiornato al 31/03/2009
- con le modalità, nei termini e con le clausole di cui alla relazione del Responsabile del CED aziendale e all'offerta della ditta medesima citate in narrativa che qui si approvano e si allegano alla presente deliberazione quale parte integrante e sostanziale della stessa;
2. di contabilizzare il costo derivante dall'adozione della presente deliberazione pari a € 14.400,00 (IVA compresa) nel Bilancio ASL della Provincia di Varese - gestione sanitaria - Esercizio 2009 - Conto 10110420;
  3. di dare atto che il presente provvedimento non è soggetto a controllo preventivo e che il medesimo è immediatamente esecutivo giusta art. 13, comma 7, Legge Regionale 11 luglio 1997 n. 31, disponendone la pubblicazione e la trasmissione in copia al Collegio Sindacale dell'Azienda.

IL DIRETTORE GENERALE  
(Dr. Pierluigi Zeli)

IL DIRETTORE AMMINISTRATIVO  
(Dr. Massimo Lavessi)

IL DIRETTORE SANITARIO  
(Dr. Elio Giorgio Marmondi)

*Elio Marmondi*

000010



Copia del presente atto è stata trasmessa al Collegio Sindacale in data

\_\_\_\_\_

=====

Il presente provvedimento è stato rassegnato alla Conferenza dei Sindaci con nota

\_\_\_\_\_

=====

Il presente provvedimento è stato trasmesso alla Giunta Regionale con nota

n. \_\_\_\_\_ del \_\_\_\_\_ Esito esame Giunta Regionale: \_\_\_\_\_

=====

**CERTIFICATO DI PUBBLICAZIONE**

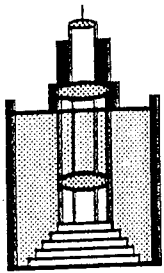
12 GEN. 2009

La presente deliberazione è stata pubblicata nei modi di legge dal \_\_\_\_\_

Varese, 12 GEN. 2009

IL FUNZIONARIO DELEGATO  
Dr. Antonio Grimaldi

=====



**A.S.L.**  
Azienda  
Sanitaria  
Locale  
della  
Provincia di  
**VARESE**

Istituita con  
D.P.G.R.  
n. 70640 del  
22.12.1997

Prot. n. 2008/014SI0014665/1


**DIREZIONE GENERALE**  
**Ufficio Sistema Informativo – CED**  
Via O. Rossi, 9 - 21100 Varese  
Tel. 0332/277207 Fax 0332/277422

Varese, 26/11/2008

**ALLEGATO DELIBERAZIONE**  
**N. 2 DEL 9 GEN. 2009**  
**COMPOSTA DA N. 6 FOGLI**

Al Direttore Generale  
Dr. Pierluigi Zeli

Al Direttore Amministrativo  
Dr. Massimo Lavessi

e, p.c.  Al Responsabile  
Servizio Affari Generali e Legali  
Dr.ssa Gabriella Broggi

Al Responsabile  
Servizio Gestione Approvvigionamenti  
Ing. Alessandro Radice

Loro Sedi

**Oggetto:** Richiesta di affidamento per l'anno 2008 della consulenza informatica per l'attuazione del Decreto Legislativo 196/2003 riguardante il Codice in materia di Protezione dei Dati Personali – Precisazioni

Nelle more dell'espletamento delle procedure di gara per rinnovare la Consulenza informatica in atto, per garantire a questa ASL la continua e regolare attuazione del Decreto Legislativo 196/2003 riguardante il Codice in materia di Protezione dei Dati Personali, si trasmette il parere dello scrivente sulla proposta di affidamento all'Impresa GFI Italia, che collabora con l'ASL per le attività concernenti la sicurezza informatica.

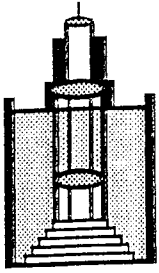
Si sottolinea inoltre, che la tematica di riferimento coinvolge anche il Servizio Affari Generali e Legali cui compete di sovrintendere all'attuazione del Codice per gli aspetti generali e per gli aspetti specifici connessi al trattamento dei dati sensibili, comuni e giudiziari registrati su supporto cartaceo.

L'allegata offerta tecnica ed economica, Prot. n. 2008/014P0109113 del 7/11/2008, propone l'effettuazione di attività finalizzate al raggiungimento di tre precisi obiettivi:

1. Realizzazione dell' "Allegato A - Analisi dei Rischi" da allegare al DPS aggiornato al 31/03/2008 (già presente in ASL e oggetto di delibera n. 211 del 31/03/2008)
2. Realizzazione delle due Procedure seguenti che andranno ad aggiungersi al nuovo DPS aggiornato al 31/03/2009:
  - a. Procedura della gestione degli Account automatica e centralizzata presso il CED, nell'ambito di un regolamento dedicato al personale di questa struttura
  - b. Procedura di analisi sistemistica dei log e di controllo degli accessi presso il CED, nell'ambito di un regolamento dedicato al personale di questa struttura.

Sede Legale: Via Ottorino Rossi, 9 - 21100 VARESE - Tel. 0332/277.111 - Fax 0332/277.413  
C. F. e P. IVA 02413470127





**A.S.L.**  
Azienda  
Sanitaria  
Locale  
della  
Provincia di  
**VARESE**

Istituita con  
D.P.G.R.  
n. 70640 del  
22-12-1997

3. Realizzazione dell' "Allegato A - Analisi dei Rischi" da allegare al DPS aggiornato al 31/03/2009

In relazione al fatto di affidare tali attività all'Impresa GFI Italia, si esprime un parere favorevole all'accettazione della relativa offerta per i seguenti motivi:

- continuità del servizio già erogato a partire dall'affidamento originale della consulenza avvenuto nell'anno 2004, nelle modalità tecniche ed organizzative (utilizzo della metodologia CRAMM) già adottate dal personale dell'impresa GFI nelle precedenti analisi dei rischi e relativa identificazione delle misure di sicurezza da realizzare per la loro eliminazione
- sostanziale soddisfazione per quanto finora realizzato con la collaborazione del personale dell'ASL competente in materia
- congruità dell'offerta economica nel rapporto costo/benefici, pari ad € 12.000,00 oltre iva, ritenuta corrispondente all'impegno previsto e allineata alle tariffe di mercato

Sotto l'aspetto contabile i costi della consulenza richiesta sono da assegnare al Centro di Costo del CED C21012010 e da registrare nel Conto Economico 10110420 - Consulenze e Collaborazioni amministrative.

In attesa dell'approvazione della presente richiesta, si resta a disposizione per ogni utile chiarimento.

Cordiali saluti.

IL DIRIGENTE INGEGNERE  
RESPONSABILE C.E.D.  
Ing. Marco Pelizzari



Responsabile Procedimento: Ing. Marco Pelizzari  
Responsabile Istruttoria: Ing. Marco Pelizzari

Sede Legale: Via Ottorino Rossi, 9 - 21100 VARESE - Tel. 0332/277.111 - Fax 0332/277.413  
C. F. e P. IVA 02413470127





## Stima dei rischi

L'obiettivo di questa attività è valutare i rischi ai quali può essere esposto il sistema, attraverso un'analisi delle minacce, delle vulnerabilità e del valore delle risorse (calcolato in precedenza).

Le attività da svolgere sono:

- riesaminare le minacce, e le vulnerabilità ad esse relative, alla luce degli eventuali cambiamenti tecnologici intervenuti;
- valutare il livello delle minacce e il grado di vulnerabilità delle risorse rispetto alle minacce.

La valutazione delle minacce e delle vulnerabilità è fatta tramite questionari all'uopo predisposti da CRAMM. Per ogni minaccia identificata viene erogato un questionario: le risposte fornite dall'intervistato determineranno il livello della minaccia su una scala qualitativa del tipo molto bassa, bassa, media, alta, molto alta, ed il livello della vulnerabilità su una scala qualitativa del tipo bassa media, alta.

Dopo aver valutato le risorse ed analizzato le minacce e le vulnerabilità, è possibile valutare i rischi. La valutazione è effettuata attraverso una scala di valori da 1 a 7 utilizzando la matrice di rischio.

Per ogni risorsa (o gruppo di risorse) viene individuata una misura di rischio per ciascuna minaccia che insiste sulla risorsa stessa. Ciò è fatto in funzione di tutte le possibili combinazioni tra i livelli delle minacce e della vulnerabilità e del valore (impatto) della risorsa.

## Selezione delle misure di sicurezza

Questa attività ha l'obiettivo di selezionare le misure di sicurezza destinate a far fronte ai rischi individuati. CRAMM seleziona le opportune misure di sicurezza confrontando i rischi associati a ciascuna minaccia individuata con il livello di sicurezza che la misura è in grado di soddisfare.

## Aggiornamento degli archivi

Parallelamente all'attività di cui sopra si procederà all'aggiornamento degli archivi contenenti dati sensibili e/o giudiziari; conseguentemente, saranno altresì aggiornati gli strumenti hardware e software necessari al loro trattamento.

## Redazione procedure

Verranno redatte le seguenti procedure:

1. Procedura della gestione degli Account automatica e centralizzata presso il CED., nell'ambito di regolamento dedicato al personale di questa struttura,
2. Procedura di analisi sistemistica dei log e di controllo degli accessi presso il CED., nell'ambito di regolamento dedicato al personale di questa struttura.



## Gruppo di lavoro e tempi

Per la realizzazione delle attività di cui ai precedenti capitoli si ritiene necessario l'impegno di un Senior Security Consultant, Lead Auditor ISO/IEC 27001, e di Senior Security Specialist.

Le attività saranno realizzate entro 50 giorni solari dall'inizio dei lavori compatibilmente con la disponibilità del personale dell'Azienda da incontrare.

Le attività saranno svolte in parte presso la sede dell'Azienda ed in parte presso gli uffici di Gfi Italia.



## OFFERTA ECONOMICA

Il prezzo dell'intervento a valutato a corpo in € 12.000,00 (Dodicimila/00 Euro), al netto degli oneri di legge e comprensivo delle spese di trasferta.  
Nell'importo è compreso anche il secondo allegato A per il DPS da aggiornare al 31/03/2008.

## DIRITTI E RISERVATEZZA

La GFI Italia S.p.A. si impegna formalmente, e impegna il nostro personale, a non divulgare notizie o informazioni di carattere riservato acquisite durante l'espletamento delle attività oggetto della presente offerta.

## CONDIZIONI DI FORNITURA

Validità offerta	30 Novembre 2008
Fatturazione:	40% all'ordine 60% fine attività
Forma di pagamento:	Bonifico Bancario
Termini di pagamento:	90 giorni data fattura fine mese
Oneri fiscali:	a Vostro carico



*[Handwritten signature]*



## Premessa

L'oggetto della presente offerta si sostanzia in un'attività di consulenza destinata alla realizzazione dell'analisi dei rischi finalizzata all'aggiornamento del Documento Programmatico sulla Sicurezza (DPS) della ASL di Varese (nel seguito, Azienda) e all'aggiornamento degli archivi contenenti dati sensibili e/o giudiziari. L'attività di analisi dei rischi sarà realizzata con l'ausilio della metodologia CRAMM, già utilizzata nel corso dei precedenti interventi.

## Aggiornamento dell'analisi dei rischi

### Aggiornamento dei modelli delle risorse

Questa attività ha l'obiettivo di aggiornare i modelli delle risorse (asset model) definiti nel corso del precedente intervento. L'aggiornamento si rende necessario in virtù degli eventuali cambiamenti tecnologici che sono intervenuti nel trattamento degli archivi contenenti dati personali sensibili e/o giudiziari. Secondo la metodologia CRAMM, infatti, l'asset model serve a descrivere i legami esistenti tra gli archivi di dati e le risorse hardware e software necessarie al trattamento quotidiano dei dati stessi.

### Valutazione delle risorse

In funzione dei risultati derivanti dalla precedente attività si procederà alla valutazione delle risorse (dati, hardware e software) sulla falsariga di quanto fatto nel corso del precedente intervento. In particolare, i valori delle risorse sono determinati tramite interviste in cui viene chiesto di descrivere le possibili conseguenze derivanti da diversi tipi d'impatto:

- indisponibilità;
- distruzione;
- scoperta;
- modifiche;
- ecc..

Lo scenario d'impatto delineato dall'intervistato va poi confrontato con quelli presenti nelle linee guida di CRAMM. Esempi di scenari d'impatto sono:

- Violazione di informazioni personali (privacy);
- Perdite finanziarie;
- Perdita di immagine;
- Violazioni di Obblighi di legge e/o regolamenti;
- Riduzione dell'operatività aziendale.

