# CODICE DELLA PRIVACY

***(D.L.vo N. 196/2003)***

**DISPOSIZIONI MINIME SULLA SICUREZZA**

**E**

**DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

Il presente documento si compone di n. 31 pagine (inclusa la presente e gli allegati)

Data di emissione: <emissione>

Il responsabile della sicurezza

F.to Fabio Lizzi



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**

P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y

Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007

Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

# Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

**<ragsoc>**
<ragsoc2>
<indirizzo>
<cap> <localita> <provincia>

## Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato da <ragsoc>, previsti dal D.L.vo 30/06/2003 Num. 196 "Codice in materia di protezione dei dati personali".
Il presente documento è stato redatto da <redattore>. in qualità di <redattorequalifica>, che provvede a firmarlo in calce.
Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

## Normativa di riferimento

D.L.vo n. 196 del 30/06/2003;
Regolamento per l'utilizzo della rete.

## Definizioni e responsabilità

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.
Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è <titolare> e la titolarità è esercitata dal rappresentante legale, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

## Titolare, responsabili, incaricati

Titolare del trattamento: <titolare>
Responsabile del trattamento dei dati: <trattamento>



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

Responsabile della sicurezza informatica: <sicurezza>
Amministratore della rete: <amministratore>
Custode delle password: <custodepassword>
Incaricati del trattamento dei dati: come da allegato 1
Incaricato dell'assistenza e della manutenzione degli strumenti elettronici: <assistenza>

## Analisi dei rischi

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.
L'analisi dei rischi consiste nella:
individuazione di tutte le risorse del patrimonio informativo;
identificazione delle minacce a cui tali risorse sono sottoposte;
identificazione delle vulnerabilità;
definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

## Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;

Per ulteriori dettagli vedere gli Allegati 1 e 3.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

## Individuazione delle minacce

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse.

| Rischi | Deliberato | Accidentale | Ambientale |
|---|---|---|---|
| Terremoto | | | X |
| Inondazione | X | X | X |
| Uragano | | | X |
| Fulmine | | | X |
| Bombardamento | X | X | |
| Fuoco | X | X | |
| Uso di armi | | X | |
| Danno volontario | X | | |
| Interruzione di corrente | | X | |
| Interruzione di acqua | | X | |
| Interruzione di aria condizionata | X | X | |
| Guasto hardware | | X | |
| Linea elettrica instabile | | X | X |
| Temperatura e umidità eccessive | | | X |
| Polvere | | | X |
| Radiazioni elettromagnetiche | | X | |
| Scariche elettrostatiche | | X | |
| Furto | X | | |
| Uso non autorizzato dei supporti di memoria | X | | |
| Deterioramento dei supporti di memoria | | X | |
| Errore del personale operativo | | X | |
| Errore di manutenzione | | X | |
| Masquerading dell'identificativo dell'utente | X | | |
| Uso illegale di software | X | X | |
| Software dannoso | | X | |
| Esportazione/importazione illegale di software | X | | |
| Accesso non autorizzato alla rete | X | | |
| Uso della rete in modo non autorizzato | X | | |



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

| | | | |
|---|---|---|---|
| Guasto tecnico di provider di rete | | X | |
| Danni sulle linee | X | X | |
| Errore di trasmissione | | X | |
| Sovraccarico di traffico | X | X | |
| Intercettazione (Eavesdropping) | X | | |
| Infiltrazione nelle comunicazioni | X | | |
| Analisi del traffico | | X | |
| Indirizzamento non corretto dei messaggi | | X | |
| Reindirizzamento dei messaggi | X | | |
| Ripudio | X | | |
| Guasto dei servizi di comunicazione | X | X | |
| Mancanza di personale | | X | |
| Errore dell'utente | X | X | |
| Uso non corretto delle risorse | X | X | |
| Guasto software | X | X | |
| Uso di software da parte di utenti non autorizzati | X | X | |
| Uso di software in situazioni non autorizzate | X | X | |

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 2

## Individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 6.

| Infrastruttura | Hardware | Comunicazioni |
|---|---|---|
| Mancanza di protezione fisica dell'edificio (porte finestre ecc.) | Mancanza di sistemi di rimpiazzo | Linee di comunicazione non protette |
| Mancanza di controllo di accesso | Suscettibilità a variazioni di tensione | Giunzioni non protette |
| Linea elettrica instabile | Suscettibilità a variazioni di temperatura | Mancanza di autenticazione |
| Locazione suscettibile ad allagamenti | Suscettibilità a umidità, polvere, sporcizia | Trasmissione password in chiaro |
| | Suscettibilità a radiazioni | Mancanza di prova di |



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

| | | |
|---|---|---|
| | elettromagnetiche | ricezione/invio |
| | Manutenzione insufficiente | Presenza di linee dial-up (con modem) |
| | Carenze di controllo di configurazione (update/upgrade dei sistemi) | Traffico sensibile non protetto |
| | | Gestione inadeguata della rete |
| | | Connessioni a linea pubblica non protette |

| Documenti cartacei | Software | Personale |
|---|---|---|
| Locali documenti non protetti | Interfaccia uomo-macchina complicata | Mancanza di personale |
| Carenza di precauzioni nell'eliminazione | Mancanza di identificazione / autenticazione | Mancanza di supervisione degli esterni |
| Non controllo delle copie | Mancanza del registro delle attività (log) | Formazione insufficiente sulla sicurezza |
| | Errori noti del software | Mancanza di consapevolezza |
| | Tabelle di password non protette | Uso scorretto di hardware/software |
| | Carenza/Assenza di password management | Carenza di monitoraggio |
| | Scorretta allocazione dei diritti di accesso | Mancanza di politiche per i mezzi di comunicazione |
| | Carenza di controllo nel caricamento e uso di software | Procedure di reclutamento inadeguate |
| | Permanenza di sessioni aperte senza utente | |
| | Carenza di controllo di configurazione | |
| | Carenza di documentazione | |
| | Mancanza di copie di backup | |
| | Incuria nella dismissione di supporti riscrivibili | |

## Individuazione delle contromisure



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

**Contromisure di carattere fisico**

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità di (indircare il responsabile)
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura di ;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'ENTE, DITTA O PERSONA FISICA……;
- i locali sono provvisti di sistema di allarme e di estintore (indicare se le misure sono attive o entro quando lo saranno);
- sono programmati interventi atti a dotare i locali ad accesso controllato di porte blindate, armadi ignifughi, impianti elettrici dedicati, sistemi di condizionamento, apparecchiature di continuità elettrica (indicare quali interventi sono attivi, quali programmati).

**Contromisure di carattere procedurale**

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in  e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro.
- il responsabile del trattamento dei dati è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla ditta ;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato (indicare il luogo)

**Contromisure di carattere elettronico/informatico**
Vedere l'Allegato 3.

## Norme per il personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

## Incident response e ripristino

Vedere l'Allegato 3

## Piano di formazione

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:
- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

## Aggiornamento del piano

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della ditta ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo della ditta tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

### *Elenco Allegati costituenti parte integrante di questo documento*

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Il redattore del documento

F.to Fabio Lizzi

*Nota: Fonti di documentazione*
*Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:*

- **http://www.garanteprivacy.it**
- *"Sicurezza informatica" ECDL IT Administrator - Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1*
- *Il regolamento per l'utilizzo della rete è stato derivato dal documento CISEL 0203G286 - CISEL Centro Studi per gli Enti Locali - Maggioli*



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

## ALLEGATO 1 – Elenco trattamenti dei dati

**Tabella 1 - Elenco dei trattamenti dei dati**

| Finalità perseguita o attività svolta | Categorie di interessati | Natura dei dati trattati | Struttura di riferimento | Altre strutture che concorrono al trattamento | Descrizione degli strumenti utilizzati |
|---|---|---|---|---|---|
| Dottore Commercialista | Piccole e Medie Imprese | Dati Personali semplici | Struttura semplice composta da n. 1 Professionista | Struttura semplice composta da n. 1 Professionista | I dati vengono trattati sia con strumenti informatici che su supporto cartaceo |
| Revisore dei Conti | Piccole e Medie Imprese | Dati Personali semplici | Struttura semplice composta da n. 1 Professionista | Struttura semplice composta da n. 1 Professionista | I dati vengono trattati su supporto informatico e cartaceo |
| Consulenza Finanziaria | Piccole e Medie Imprese | Dati Personali semplici | Struttura semplice composta da n. 1 Professionista | Struttura semplice composta da n. 1 Professionista | I dati vengono solo trattati in cartaceo e vengono consegnati al Cofidi Calalbria che è il responsabile del trattamento e viene autorizzato ai sensi dell'art. 13 del D.lgs 296/2003 |

**Descrizione sintetica**: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. gestione del personale , gestione collaboratori, gestioni clienti, gestioni fornitori, ecc.) e delle categorie di persone cui i dati si riferiscono (personale, collaboratori, clienti, fornitori, ecc.).

**Natura dei dati trattati**: indicare la classe di rischio dei dati trattati tenendo presente la seguente classificazione:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio;
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

**Struttura di riferimento**: indicare la struttura (segreteria amministrativa, direzione, funzione svolta, ecc.) all'interno della quale viene effettuato il trattamento.

**Altre strutture che concorrono al trattamento**: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

dall'esterno.

**Descrizione degli strumenti utilizzati**: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi) e altre tipologie di contenitori (es. armadi, schedari…).



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

**Tabella 2 - Descrizione della struttura organizzativa**

| Struttura | Trattamenti effettuati dalla struttura | Descrizione dei compiti e delle responsabilità della struttura |
|---|---|---|
| Struttura semplice composta da n. 1 Professionista | Atttività di consulenza tipiche del Dottore Commercialista unita alla consulenza finanziaria offerta tramite il Cofidi Calabria | L'attività viene svolta dal Dott. Fabio Lizzi consiste nell'effettuare revisioni contabili, consulenze in materia fiscale, trasmissioni telematiche di dichiarazioni fiscali con Entratel e di pratiche telematiche con telemaco infocamere. Per la consulenza finanziaria consiste nel curare i rapporti e fornire assistenza ai vecchi e nuovi soci del Cofidi Calabria in collaborazione con la struttura regionale, ancha consulenze on -line tramite il modulo di contatto sul sito aziendale http://www.fabiolizzi.it |

**Struttura**: riportare le indicazioni delle strutture menzionate nella Tabella 1.

**Trattamenti effettuati dalla struttura**: indicare i trattamenti di competenza di ciascuna struttura.

**Compiti e responsabilità della struttura**: descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

**Tabella 3 - Elenco del personale incaricato del trattamento in ogni struttura e delle dotazioni informatiche.**

| Cognome e Nome | Struttura di riferimento | Strumenti utilizzati | Responsabilità aggiuntive |
|---|---|---|---|
| Dott. Fabio Lizzi | Struttura semplice composta da n. 1 Professionista | Vengono utilizzati strumenti informatici n. 2 PC (1 Desktop ed 1 Notebook) e viene raccolta ed archiviata copia cartacea dei documenti. | Le responsabilità aggiuntive riguardano principalmente la riservatezza delle notizie e documenti dei clienti in possesso considerato che per avviare una pratica di garanzia o per una semplice consulenza il cliente fornisce atti al fine di individuare e valutare il proprio patrimonio personale o quello aziendale |

**Nome e cognome:** riportare le indicazioni per ogni incaricato del trattamento.

**Struttura di riferimento:** riportare l'indicazione della struttura di appartenenza di ogni incaricato.

**Strumenti utilizzati:** per ogni incaricato riportare le informazioni relative allo strumento utilizzato (p.e. numero di inventario del PC).

**Responsabilità aggiuntive:** indicare le eventuali responsabilità aggiuntive rispetto all' incarico per il trattamento dei dati, ad esempio "responsabile del trattamento", "responsabile delle copie di backup", "custode delle chiavi di un contenitore o armadio", "custode delle password", ecc.

Nota: *parte delle indicazioni sono tratte dalla "Guida operativa per redigere il documento programmatico sulla sicurezza (DPS)" pubblicate dal garante*



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

## ALLEGATO 2 – Minacce

### Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

### Minacce a cui sono sottoposte le risorse connesse in rete

Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:
all'utilizzo della LAN/Intranet (interne);
ai punti di contatto con il mondo esterno attraverso Internet (esterne);

- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

**IP spoofing**
L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

**Packet sniffing**
Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

**Port scanning**
Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

**Highjacking**
Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.

**Social engineering**



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

**Buffer overflow**

Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

**Spamming**

Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

**Password cracking**

Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

**Trojan**

Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

**Worm**

Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

**Logic bomb**

Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

**Malware e MMC (Malicious Mobile Code)**

Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

**DOS (Denial of Service)**

Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

**DDOS (Distributed Denial of Service)**

Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti esterne a quella della rete loca LAN.

La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

**Minacce a cui sono sottoposti i dati trattati**
Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

**Minacce a cui sono sottoposti i supporti di memorizzazione**
Le principali minacce ai supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
  - sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

## ALLEGATO 3 – Misure, incident response, ripristino

**Tabella 1 - Connettività internet**

| Connettività | Apparecchiature di comunicazione | Provider |
|---|---|---|
| Connessione Iternet con Wind | Data Card - Huawei E612 - Utilizzabile esclusivamente su pc n. 02 | Wind |

**Connettività**: indicare il tipo di connettività internet (XDSL, ISDN, PSTN).

**Apparecchiature di comunicazione:** indicare il tipo di apparecchiature utilizzate per la connettività (modem, router).

**Provider**: indicare il fornitore di connettività.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

**Tabella 2 - Descrizione Personal Computer**

| Identificatico del PC | Tipo PC | Sistema operativo | Software utilizzato | Rete |
|---|---|---|---|---|
| 01 | Computer Desktop Collegato a Stampante e Scanner | Windows XP Professional | AVG Antivirus - Open Office | Nessuna |
| 02 | Notebook Asus X51RL series | Windows Vista - Home edition | Office 2003 Small Business - Entratel - Fedra Plus - AVG Antivirus - Software compilativo Agenzia Entrate - Dike - Privacy DPS - Media db Free (ware per contabilità) | |

**Identificativo del PC:** indicare l'elenco di tutti i PC utilizzati sia connessi che non connessi alla rete (per esempio con il numero di inventario).

**Tipo PC**: indicare il tipo del PC.
**Sistema operativo**: indicare quale Sistema operativo è utilizzato sul PC.

**Software utilizzato**: indicare il software applicativo utilizzato per il lavoro (es. OFFICE, STAROFFICE, ecc…).

**Rete**: indicare se il PC è connesso alla rete.

## Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- Il server non viene utilizzato con configurazioni di ridondanza;
- presenza di gruppi di continuità elettrica non necessaria inquanto il pc principale è un notebook quindi dotato di batteria;
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese (indicare se la misura è attiva o entro quando sarà adottata). Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati;
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet (indicare se la misura è attiva o entro quando sarà adottata);
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP, di seguito specificate (indicare se la misura è attiva o entro quando sarà adottata);
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria (indicare se la misura è attiva e quale prodotto è utilizzato o entro quando sarà adottata);
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate

## Regole per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.
User-id e password iniziali sono assegnati, dal custode delle password.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
La User-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.
La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
per la definizione/gestione della password devono essere rispettate le seguenti regole:
- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere lo user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia

## Regole per la gestione di strumenti elettronico/informatico

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su …(indicare il dispositivo, CD, cassetta, ecc…) sono conservate in…(specificare il tipo di contenitore es. armadio chiuso a chiave , e indicare la sua ubicazione)
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
- Il fax si trova in locale ad accesso controllato (specificare dove) e l'utilizzo è consentito unicamente agli incaricati del trattamento (specificare chi)

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

## Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- *divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;*
- *limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;*
- *controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;*
- *evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;*
- *disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;*
- *disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);*
- *attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);*
- *non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");*
- *non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);*
- *non utilizzare le chat;*
- *consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;*
- *non attivare le condivisioni dell'HD in scrittura.*
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk,definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

## Incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.



Via R. A. Livatino, 5 – 88900 Crotone (KR) – Tel 347.37.87.011 – **info@fabiolizzi.it http://www.fabiolizzi.it**
P.Iva 02851680799 C.F. LZZ FBA 76P23 D122Y
Albo dei Dottori Commercialisti per la Circoscrizione del Tribunale di Crotone n.245 dal 04 Aprile 2007
Registro dei Revisori Contabili n.144751 - D.M.30/05/2007 Pubblicato sulla G.U. 4 Serie Speciale n.47 del 16/06/2007