

Metti al sicuro il tuo Business. Vademecum per la sicurezza dei dati

Paola Generali, *Vice Presidente e
Coordinatrice GdL Sicurezza Informatica di Assintel*



ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESI ICT

Metti al sicuro il tuo business



ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

Metti al sicuro il tuo
BUSINESS
Vademecum per la sicurezza dei dati aziendali

SCARICALO GRATUITAMENTE SU
WWW.CONFCOMMERCIO.MILANO.IT



INTRODUZIONE

Le PMI e la sicurezza delle informazioni

Struttura del vademecum

1. I SISTEMI INFORMATIVI AZIENDALI

1.1 Cosa s'intende per sistemi informativi

1.2 Ruolo del sistema informativo

1.3 Outsourcing e cloud

1.4 Internet delle cose (*IoT*)

1.5 Big Data

1.6 Continuità operativa (*Business Continuity*)

1.7 e-Commerce e Social Business

2. LA SICUREZZA DEI SISTEMI INFORMATIVI

2.1 Il valore delle informazioni per l'azienda

2.2 Cosa s'intende per sicurezza delle informazioni

Disponibilità

Riservatezza

Integrità

La sicurezza, la funzionalità e la facilità d'uso

2.3 Protezione dei dati personali

2.4 Sicurezza informatica (*Cyber Security*)

2.5 Garanzie da richiedere ai fornitori esterni (*outsourcer*)

2.6 Conformità normativa (*Compliance*)

3. LA GESTIONE DEL RISCHIO

3.1 Come valutare i rischi

Minacce e vulnerabilità

Valutazione dei rischi

3.2 Come affrontare i rischi

Rischi informatici e business

La gestione del rischio

Accettabilità del rischio

Cosa fare in pratica

3.3 Gestione degli utenti

3.4 Aggiornamento dei sistemi

3.5 Protezione dai codici maligni

3.6 Gestione dei siti web aziendali

3.7 Gestione della navigazione sul web

3.8 Gestione della posta elettronica

3.9 Gestione dei *social network*

3.10 Gestione dei personal computer dell'azienda

3.11 Sicurezza Mobile e *Bring your own device* (BYOD)

3.12 Creazione e gestione della rete locale e wireless in
sicurezza

Cosa è la rete locale (o LAN, o *Local Area Network*)

3.13 Gestione dei dispositivi di memorizzazione esterni

3.14 Gestione dei servizi gratuiti di *cloud storage*



3.15 Organizzazione della sicurezza: politiche e procedure

Perchè "organizzare" la sicurezza

Come "organizzare" la sicurezza

Differenze fra politiche e procedure

Politiche e procedure (non documenti con scritte le politiche e le procedure)

Esempio di gerarchia delle politiche e delle procedure

3.16 Gestione degli *outsourcer*: contratti e Service Level Agreement

La sicurezza nei contratti e SLA

Scopo e natura dei contratti e SLA nel contesto Sicurezza/Conformità

Caveat emptor (il compratore stia attento!)

Chi definisce contratti e accordi (SLA)

Contratti e accordi (SLA) non trasferiscono la responsabilità ultima di un trattamento dati

Esempio di SLA relativo alla raccolta di eventi di *log* "As A Service"

3.17 Sicurezza ITC ed impianti primari

3.18 Gestione degli incidenti

3.19 Garanzia della disponibilità delle informazioni

3.20 Formazione e sensibilizzazione degli utenti



4. LE NORME VIGENTI IN MATERIA

4.1 Il Regolamento Europeo sulla Protezione dei Dati

4.2 La legge sui *cookie* (*cookie law*)

4.3 La legge sul crimine informatico (*computer crime*)

4.4 Il Decreto Legislativo 231/2001

4.5 Il Codice dell'Amministrazione Digitale (CAD)

5. STANDARD INTERNAZIONALI PER LA GESTIONE DEI SISTEMI INFORMATIVI

5.1 ISO/IEC 27001:2013 - Sicurezza delle informazioni

5.2 ISO 22301:2012 - Gestione della continuità operativa

5.3 ISO/IEC 20000:2011 - Gestione dei servizi IT



Grazie per l'attenzione

Dott.ssa Paola Generali
Managing Director
GETSOLUTION
paola.generalis@getsolution.it
cell: 335-5366986
www.getsolution.it



 @Assintel

 GdL Assintel Sicurezza Informatica

