Politica per la Sicurezza

Linee di indirizzo aziendali per la sicurezza delle informazioni

Codice	CODIN-ISO27001-POL-01-B	Tipo	Politica
Progetto	Certificazione ISO 27001	Cliente	CODIN S.p.A.
Autore	Direttore Tecnico	Data	14 ottobre 2014
Revisione	Resp. SGSI	Approvazione	Direttore Generale
Stato	Approvato	Classificazione	Pubblico

CODIN S.p.A. – Via del Pescaccio, 30 – 00166 ROMA – E-mail: info@codin.it – Tel. +39 06 661 71 41 – Fax +39 06 6618 8640

Indice delle revisioni

Ed.	Data	Parti revisionate	Emesso	Approvato
A	15/5/2014	Intero documento	Direttore Tecnico	Direttore Generale
B	14/10/2014	Cap. 3 “Responsabilità”	Direttore Tecnico	Direttore Generale

Indice degli argomenti

1 Introduzione

Il presente documento riporta la politica aziendale definita dalla Direzione di CODIN S.p.A. in merito alla gestione delle informazioni, dei dati e degli asset fisici, al fine di garantire la sicurezza delle informazioni e dei dati trattati dall'azienda, in termini di riservatezza, integrità e disponibilità.

1.1 Scopo del documento

La Politica per la Sicurezza definisce le linee guida in base alle quali è stato definito l'intero Sistema per la Gestione della Sicurezza delle Informazioni (SGSI) di CODIN. Ogni piano e procedura inerente il trattamento delle informazioni o che possa avere impatto con la sicurezza delle informazioni, deve uniformarsi alla politica delineata nel presente documento.

1.2 Ambito

La Politica per la Sicurezza si applica a tutte le attività svolte da CODIN, ed in particolare all'attività di Product Management, ossia alle attività di progettazione, sviluppo e manutenzione di prodotti software e gestione infrastrutture correlate.

1.3 Definizioni e acronimi

Di seguito sono riportate le principali definizioni e acronimi utilizzate nelle pagine del presente documento.

Definizione	Descrizione
CCNL	Contratto collettivo nazionale di lavoro
D.lgs 196/2003	Decreto legislativo in merito alla privacy e alla tutela dei dati personali
ISO 27001	Norma internazionale che definisce i requisiti per l'impostazione di un SGSI
NDA	Non Disclosure Agreement, accordo di riservatezza
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SLA	Service Level Agreement, dichiarazione del livello di servizio offerto nell'ambito della fornitura di un servizio

Tabella 1: Definizioni e acronimi

1.4 Riferimenti

Nell'ambito del presente progetto sono a disposizione i seguenti documenti:

[1] CODIN, *Manuale del Sistema di Gestione della Sicurezza delle Informazioni*, 2014.

[2] CODIN, *Piano di Sicurezza Logica*, 2014.

[3] CODIN, *Piano di Sicurezza Fisica*, 2014.

[4] CODIN, *Regolamento Aziendale*, 2014.

[5] CODIN, *Procedura di controllo degli accessi*, 2014.

[6] UNI, *ISO/IEC 27001:2013*.

[7] D.lgs 196/2003, *Codice in materia di protezione dei dati personali*.

Sono inoltre disponibili i seguenti riferimenti on-line:

[8] ISO – Sito Istituzionale: http://www.iso.org/iso/home.html

[9] ISO 27001 – Information Security Management: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[10] ISO/IEC 27001 su Wikipedia: http://it.wikipedia.org/wiki/ISO/IEC_27001

1.5 Organizzazione del documento

Il documento è articolato su tre capitoli, compreso questo capitolo introduttivo.

Nel Capitolo 2 vengono definiti i principi che costituiscono la Politica per la Sicurezza di CODIN; nel Capitolo 3 vengono delineate le responsabilità che rientrano nella competenza di diverse figure presenti nell'organizzazione aziendale.

2 Politica

Di seguito sono riportate le policy definite da CODIN in merito alla sicurezza delle informazioni.

2.1 Accettazione

Dipendenti, collaboratori, fornitori, partner, appaltatori e tutte le altre terze parti coinvolti nelle attività istituzionali di CODIN devono accettare i loro obblighi e le responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse di CODIN o affidati a CODIN da terzi.

2.2 Accesso

Accesso alle informazioni, beni e risorse della CODIN o affidati a CODIN da terzi, devono essere controllati e monitorati sulla base dei seguenti criteri:

- L'accesso è autorizzato solo per le informazioni necessarie (principio della conoscenza minima o *need to know*);
- L'accesso è autorizzato solo per le informazioni riguardanti specifiche attività.

2.3 Valutazione

CODIN definisce il giusto rapporto tra:

1. le spese necessarie per l'attuazione delle misure al fine di proteggere le informazioni, i beni e le risorse di CODIN o affidati a CODIN da terzi;
2. i rischi legati all'utilizzo non autorizzato, modifiche o distruzione.

2.4 Consapevolezza

La Direzione aziendale assicura che ogni dipendente, collaboratore, fornitore o terza parte sia consapevole con la Politica per la Sicurezza di CODIN e che i suoi comportamenti e gli strumenti utilizzati siano adeguati e in linea con la politica di sicurezza di CODIN.

2.5 Formazione

La Direzione aziendale garantisce che ogni risorsa sia addestrata sulle politiche organizzative applicate e le procedure relative alla sicurezza delle informazioni.

2.6 Rispetto delle leggi e regolamenti obbligatori

Tutti i trattamenti delle informazione e le procedure per la sicurezza di CODIN sono conformi alle leggi e ai regolamenti obbligatori. La CODIN tutela la sicurezza delle informazioni nel pieno rispetto delle leggi e dei regolamenti, anche per quel che riguarda lo specifico riferimento al D.lgs 196/2003 e s.m.i. e al CCNL.

CODIN si impegna altresì a mantenere un inventario delle licenze software acquistate dall'azienda e a verificare periodicamente l'uso di software con diritti di licenza da parte dei propri dipendenti e collaboratori, contrastando la violazione di tali diritti.

2.7 Protezione

Tutte le informazioni, beni e risorse di CODIN o affidate da CODIN da terzi parti sono protette contro i rischi legati al rispetto della riservatezza, dell'integrità e della disponibilità in proporzione al loro valore e in conformità con le leggi vigenti.

Le registrazioni rilevanti sono protette da perdita, distruzione, falsificazione, accessi e divulgazione non autorizzati, in conformità con i requisiti legali, normativi, contrattuali e di business, attraverso appositi strumenti tecnici e procedure operative descritte nel Piano di Sicurezza Fisica, nel Piano di Sicurezza Logica e nella Procedura di controllo degli accessi.

I sistemi informatici che utilizzino canali di comunicazione pubblici (es.: rete Internet) sono configurati per eseguire la cifratura e la decifratura delle informazioni trasmesse. Per comunicazioni tra sistemi interni le chiavi crittografiche possono essere generate dai sistemi dedicati a tale operazione a cura dell'Area dei Sistemi Informativi Aziendali. Le chiavi crittografiche utilizzate su sistemi che comunicano con terze parti, sono generate e gestite da Certification Authority esterne. Entrambe le modalità garantiscono il medesimo livello di protezione, garantendo l'autenticità, la riservatezza e l'integrità delle informazioni trasmesse. Il processo di gestione del ciclo di vita delle chiavi crittografiche, a cura dell'Area dei Sistemi Informativi Aziendali, è descritto nel Piano di Sicurezza Logica.

L'uso di strumenti crittografici viene attuato nell'ambito del pieno rispetto della normativa vigente e in conformità con regolamenti ed accordi con terze parti.

I sistemi utilizzati per la gestione di informazioni aziendali sono dislocati in locali sicuri, ad accesso controllato. La protezione è garantita da apposite contromisure per prevenire la violazione della riservatezza e della integrità sia fisica che logica, descritte rispettivamente nel Piano di Sicurezza Fisica e nel Piano di Sicurezza Logica.

CODIN adotta una politica di separazione degli ambienti IT dedicati allo sviluppo, al test/collaudo e all'esercizio dei propri sistemi informativi, al fine di ridurre i rischi di accesso non autorizzato alle informazioni e di modifiche o di indisponibilità dei sistemi di esercizio.

È tutelata la sicurezza delle informazioni che vengono gestite al di fuori del sistema informativo aziendale, attraverso specifiche politiche di comportamento comunicate attraverso il Regolamento Aziendale.

2.8 Sicurezza nella progettazione e sviluppo di soluzioni IT

CODIN adotta un insieme di strumenti descritti nel Piano di Sicurezza Logica e nel Piano di Sicurezza Fisica, per garantire la sicurezza del processo di sviluppo, al fine di assicurare

l'integrità, la disponibilità e la riservatezza dei deliverable realizzati nell'ambito di tale processo.

2.9 Relazioni con i fornitori

CODIN adotta la politica di responsabilizzare i propri fornitori e le terze parti con cui collabora per le proprie attività, mediante specifici accordi di *non disclosure agreement*.

Gli indicatori SLA e gli accordi NDA con i fornitori sono rivisti periodicamente e comunque a valle di ogni revisione della valutazione dei rischi.

3 Responsabilità

Le responsabilità di cui al presente capitolo sono generali e riguardano l'intera organizzazione di CODIN.

Tutti devono:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di CODIN o affidate a CODIN da terze parti;
- proteggere i beni materiali, i sistemi informatici e le risorse di CODIN o affidati a CODIN da terze parti;
- proteggere ogni informazione, attività e risorsa sotto la propria responsabilità;
- contattare la Direzione, le autorità competenti e/o adeguate in caso di violazioni della sicurezza effettive o presunte;
- contattare la Direzione e il Responsabile della Sicurezza, in caso di qualsiasi modifica necessaria della politica di sicurezza, dei requisiti di sicurezza, degli standard, delle procedure.

La violazione dei principi e dei comportamenti a tutela della sicurezza delle informazioni saranno perseguite da CODIN in misura proporzionata alla gravità delle infrazioni commesse ed in linea con quanto stabilito dal CCNL CONFAPI, dal D.Lgs.196/03 (Codice in materia di protezione dei dati personali) e dal "*Modello di Organizzazione, Gestione e Controllo*" che CODIN ha implementato ai sensi del D.Lgs.231/2001.

I Responsabili delle Unità Organizzative devono:

- essere in linea con la politica di sicurezza, i requisiti, gli standard e le procedure definite;
- identificare e definire i diritti di accesso delle risorse per le loro attività e responsabilità specifiche;
- richiedere alle terze parti di essere in linea con gli accordi di riservatezza (accordo di non divulgazione);
- definire un livello di rischio accettabile in seguito alla realizzazione di una valutazione dei rischi;
- vigilare sull'adempimento di quanto previsto dalla Politica per la sicurezza da parte dei propri dipendenti.

Il Responsabile del SGSI deve :

- garantire e monitorare il rispetto delle politiche di sicurezza, requisiti, norme e procedure definite;

- garantire che il personale di CODIN sia formato e consapevole sulla Politica, sui requisiti, sugli standard e sulle procedure definite per garantire la sicurezza delle informazioni e delle risorse;

Il Responsabile della Sicurezza IT deve :

- implementare la gestione della sicurezza sulla base delle politiche di sicurezza emesse da CODIN;
- rivedere le informazioni e le risorse fisiche sotto la sua responsabilità, al fine di definire il livello di controllo adeguato da attuare perché il controllo di sicurezza sia proporzionato al valore delle informazioni e delle risorse da proteggere e nel rispetto delle leggi e dei regolamenti obbligatori;
- definire i requisiti di sicurezza di cui è necessario tenere conto nella definizione del budget per il mantenimento e lo sviluppo dei sistemi informativi aziendali;
- controllare con regolarità lo stato dei sistemi informativi aziendali, per garantire la conformità con gli standard e le politiche di sicurezza di CODIN.

I Responsabili delle Unità Organizzative hanno le seguenti responsabilità:

- garantire il rispetto della legge italiana (in particolare il D.lgs 196 nel 2003) nelle attività della propria Unità Organizzativa e nel trattamento delle informazioni;
- rendere consapevoli le risorse umane afferenti alla propria Unità Organizzativa circa le conseguenze in caso di mancato rispetto della politica di sicurezza.

Qualsiasi modifica all'organizzazione o ai processi aziendali, alle strutture e ai sistemi di elaborazione delle informazioni che hanno effetto sulla sicurezza delle informazioni, deve essere valutata e autorizzata dalla Direzione Aziendale.

L'approccio di CODIN nella gestione della sicurezza delle informazioni e della sua implementazione (obiettivi dei controlli, controlli, politiche, processi e procedure per la sicurezza delle informazioni) viene rivista annualmente nell’ambito dei processi di riesame della Direzione, o in modo indipendente dalla periodicità annuale, quando intervengono cambiamenti significativi.