Politica per la Sicurezza: Linee di indirizzo aziendali per la sicurezza delle informazioni

1 Introduzione

Il presente documento riporta la politica aziendale definita dalla Direzione di Benacchio 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. 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 Benacchio, 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 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 Benacchio; nel Capitolo 3 vengono delineate le responsabilità che rientrano nella competenza di diverse figure presenti nell'organizzazione.

2 Politica

Di seguito sono riportate le policy definite da Benacchio 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 Benacchio devono accettare i loro obblighi e le responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse di Benacchio o affidati a Benacchio da terzi.

2.2 Accesso

Accesso alle informazioni, beni e risorse della Benacchio o affidati a Benacchio da terzi, devono es- sere 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

Benacchio 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 Benacchio o affidati a Benacchio 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 Benacchio e che i suoi comportamenti e gli strumenti utilizzati siano adeguati e in linea con la politica di sicurezza di Benacchio.

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 BENACCHIO SRL sono conformi alle leggi e ai regolamenti obbligatori. La BENACCHIO SRL tutela la sicurezza delle informazioni nel pieno rispetto delle leggi e dei regolamenti. Benacchio 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 Benacchio o affidate da Benacchio da terzi parti sono protette contro i rischi legati al rispetto della riservatezza, dell'integrità e della disponibilità in propor- zione al loro valore e in conformità con le leggi vigenti.

Le registrazioni rilevanti sono protette da perdita, distruzione, falsificazione, accessi e divulga- zione 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 Fisi- ca, 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 comunica- zioni 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 Au- thority 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 ac- cesso 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.

Benacchio 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

Benacchio 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

2.9 Relazioni con i fornitori

BENACCHIO SRL 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 Benacchio.

Tutti devono:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di Benacchio o affidate a Benacchio da terze parti;
- proteggere i beni materiali, i sistemi informatici e le risorse di Benacchio o affidati a Benacchio 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 misura proporzionata alla gravità delle infrazioni commesse e dal "*Modello di Organizzazione, Gestione e Controllo*" che Benacchio 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 defini- te;
- 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 BENACCHIO SRL sia formato e consapevole sulla Politica, sui requi- siti, sugli standard e sulle procedure definite per garantire la sicurezza delle informazio- ni e delle risorse;

Il Responsabile della Sicurezza IT deve :

- implementare la gestione della sicurezza sulla base delle politiche di sicurezza emesse da BENACCHIO SRL;
- 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 proporzio- nato 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 con- formità con gli standard e le politiche di sicurezza di BENACCHIO SRL.

I Responsabili delle Unità Organizzative hanno le seguenti responsabilità:

- garantire il rispetto della legge italiana 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 va- lutata e autorizzata dalla Direzione Aziendale.

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