POLITICA PER LA QUALITA'E SICUREZZA DELLE INFORMAZIONI	
Data Documento: 18/04/2017	**Versione documento: 01**

Verifica: maggiori cambiamenti rispetto alle precedenti revisioni:

§ 1; § 3.3

SOMMARIO

Ifin Sistemi Srl a socio unico
Via G. Medici 9/a
35138 Padova – Italia
Tel (+39) 049/5001500
Fax (+39) 049/5001692
Web: www.ifin.it
Mail: ifin@ifin.it
P.Iva/C.F. 01071920282

1. MISSION DELL'AZIENDA

Ifin Sistemi è una software house che si pone come mission:

1. Lo sviluppo e la fornitura di software per la conservazione dei documenti informatici, per la fatturazione elettronica verso la PA e la pre-elaborazione dei documenti.
2. La fornitura di servizi di fatturazione elettronica verso la PA.
3. La fornitura di servizi di consulenza tecnica e normativa in materia di archiviazione, processi di gestione documentale e conservazione dei documenti informatici.
4. La fornitura del servizio di conservazione dei documenti informatici di soggetti pubblici e soggetti privati.

Ifin Sistemi si prefigge come obbiettivo quello di realizzare la propria mission, seguendo standard di qualità nella realizzazione dei propri prodotti e garantendo l'aggiornamento continuo dei software con l'evoluzione dei requisiti normativi al fine di mantenere la compliance dei prodotti alle regole tecniche e alla normativa vigente.
In aggiunta, al fine di fornire i propri servizi di conservazione dei documenti informatici a enti della Pubblica Amministrazione, Ifin Sistemi ha portato a temine con successo il percorso di accreditamento come conservatore presso AgID e si pone come obbiettivo quello di garantire che il servizio proposto sia costantemente rispondente ai requisiti richiesti dall'Agenzia per l'Italia Digitale.

2. POLITICA PER LA QUALITA'

2.1. Contenuto

L'adozione di un sistema di gestione per la qualità rappresenta una decisione strategica per l'azienda e una dimostrazione della volontà di porsi in un'ottica di miglioramento continuo e di focalizzare le proprie attenzioni alla soddisfazione del cliente.
La norma EN ISO 9001:2008 prevede che il responsabile dei sistemi di gestione svolga periodicamente una "valutazione del sistema gestione qualità" tenendo chiaramente in considerazione gli obiettivi strategici espressi nella presente politica, i cambiamenti strategici di business e tecnologici accaduti e le registrazioni del sistema qualità. Tale valutazione, attuata sulla base di misurazioni oggettive, ha lo scopo di stimolare il miglioramento continuo dei processi aziendali.
La direzione condivide con il responsabile dei sistemi di gestione la metodologia da impiegare per il monitoraggio dell'intero sistema e di ogni singolo processo aziendale identificato, inoltre la direzione partecipa alla definizione dei parametri ed alla scala dei valori da impiegare per la valutazione dei risultati ottenuti nei diversi processi monitorati.
Tale valutazione sarà ponderata anche rispetto al valore del business di ogni processo e dovrà identificare chiaramente le azioni da intraprendere per il suo miglioramento da classificare secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti. Un'adeguata analisi del sistema gestione qualità dovrà inoltre essere elaborata ogni qualvolta si verifichino cambiamenti tali da incidere sul profilo e sui processi identificati e monitorati.

La politica per la qualità di Ifin Sistemi è basata sui seguenti punti fondamentali:

- Dare visibilità al mercato del proprio modo di operare.
- Strutturare la gestione di Ifin con innovative tecniche di controllo di processo, monitoraggio e gestione del personale.
- Assicurare i propri clienti e fornitori sulle reali capacità di Ifin Sistemi in termini di organizzazione e soddisfazione dei clienti finali.

2.2. Obiettivi

- Mettere in opera e mantenere un Sistema di Gestione per la Qualità certificato ISO 9001.
- Verificare periodicamente i processi aziendali al fine di migliorarne l'efficacia e l'efficienza.
- Migliorare i prodotti e i servizi offerti con lo scopo di soddisfare le sempre maggiori esigenze dei clienti.
- Adottare sistemi che permettano un'efficace comunicazione e collaborazione tra dipendenti.
- Adottare sistemi di comunicazione rivolti ai propri clienti e fornitori, tali da garantire trasparenza nell'erogazione dei servizi e un efficace scambio di informazioni allo fine di riduzione i tempi di consegna e intervento.
- Assicurare la crescita professionale delle risorse interne all'azienda attraverso:
    - Percorsi formativi.
    - Soddisfazione del personale.

2.3. Responsabilità

- **Tutto il personale** che a qualsiasi titolo collabora con l'azienda è responsabile dell'osservanza della presente policy ed è tenuto a partecipare alla segnalazione delle anomalie, anche formalmente non codificate, di cui dovesse venire a conoscenza.

- **Responsabile del Sistema di Gestione Qualità** che si occupa di**:**
    - Emanare tutte le norme necessarie ivi inclusa la classificazione e divulgazione dei documenti affinché l'organizzazione aziendale possa condurre in modo sicuro le proprie attività.
    - Raccogliere le esigenze dei capi aera per pianificare, per il personale, un percorso formativo specifico atto a garantire che il personale abbia le competenze adeguate a svolgere i compiti a lui affidati.
    - Promuovere la cultura relativa al sistema di gestione qualità.
    - Contribuire alla definizione delle contromisure da adottare a seguito di segnalazione di non conformità.

2.4. Applicabilità

La presente politica si applica indistintamente a tutti gli organi dell'azienda. L'attuazione della presente politica è obbligatoria per tutte le risorse di **Ifin Sistemi.**

3. POLITICA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

3.1. Contenuto

Le informazioni devono essere gestite in modo sicuro, accurato e affidabile e devono essere prontamente disponibili per gli usi consentiti. E' utile sottolineare che per "utilizzo dell'informazione" si intende qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.
La norma ISO IEC 27001:2013 prevede che il responsabile della sicurezza svolga periodicamente una "valutazione dei rischi" tenendo chiaramente in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi nel periodo e dei cambiamenti strategici di business e tecnologici accaduti; tale analisi dei rischi ha lo scopo di valutare il rischio di ogni asset (o beni con valore utilizzati nella tecnologia dell'informazione o comunicazione) da proteggere rispetto alle minacce individuate. La direzione condivide con il responsabile della sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella metodologia della redazione inoltre la direzione partecipa alla definizione dei parametri ed alla scala dei valori da impiegare, considerando al termine della valutazione i risultati ottenuti accettando la "soglia di rischio accettabile", il "trattamento di mitigazione dei rischi" oltre tale soglia, ed il rischio residuo a seguito del trattamento.
Tale analisi sarà ponderata anche rispetto al valore del business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere da classificare secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti. Detta analisi dovrà inoltre essere elaborata ogni qualvolta si verifichino cambiamenti tali da incidere sul profilo del rischio complessivo del sistema.

3.2. Obiettivi

L'obiettivo del sistema di gestione della sicurezza delle informazioni in **Ifin Sistemi** è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito del campo di applicazione definito (*Acquisizione, trattamento e conservazione di dati e documenti digitali*) tramite l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti. Il sistema di gestione della sicurezza delle informazioni di **Ifin Sistemi** definisce un insieme di misure organizzative e tecniche procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- **Riservatezza :** ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- **Integrità :** ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- **Disponibilità :** ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre con la presente politica, **Ifin Sistemi** intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente.
- Proteggere il proprio patrimonio informativo.
- Evitare, per quanto possibile, i ritardi nel delivery.
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità.
- Rispondere pienamente alle indicazioni della normativa vigente e cogente.
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza.

3.3. Criteri per l'identificazione della tipologia delle informazioni.

Ifin Sistemi è consapevole sia dell'importanza della tutela della riservatezza delle informazioni in generale sia che non tutte le informazioni necessitano dello stesso grado di sicurezza e segretezza del dato. Poiché l'aumento dei livelli di protezione implica un aumento nell'utilizzo di risorse e un conseguente aumento di costi Ifin Sistemi ha suddiviso le informazioni in categorie distinte ai quali applica diversi trattamenti. Ogni informazione può appartenere ad una o più categorie.

- Informazione interne ed esterne.
    - *Interne*: fanno parte di questa categoria tutte le informazioni aziendali associate al personale, alle mansioni, ai ruoli, agli strumenti aziendali necessari necessarie allo svolgimento dell'attività lavorativa quotidiana. Alle informazioni interne afferiscono anche tutti i dati clienti necessarie all'erogazione del servizio o ad attività amministrative ad esso associate.
    - *Esterne*: fanno parte di questa categoria le informazioni del cliente o di terzi, fornite dal cliente, cui Ifin Sistemi viene a conoscenza nell'erogazione del servizio richiesto. A questa categoria appartengono:
        - i documenti e dati utilizzati per il test e il collaudo degli applicativi in licenza.
        - i documenti e dati utilizzati per il debug.
        - i documenti e dati che Ifin Sistemi conserva, elabora e gestisce conto terzi nei propri impianti.
- Informazioni identificative aziendali e personali.
    - *Aziendali*: fanno parte di questa categoria le informazioni che identificano o rendono identificabile una persona giuridica (azienda), solitamente sono informazioni pubbliche.
    - *Personali*: fanno parte di questa categoria le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica. Queste a loro volta possono contenere dati il cui grado di riservatezza sia sensibilmente diverso e sono di tipo:
        - identificativi: quelli che permettono l'identificazione diretta, come i dati anagrafici;
        - sensibili: quelli che possono 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, lo stato di salute e la vita sessuale;
        - giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o di indagato.

La classificazione e la successiva modalità di trattamento dei dati per le diverse categorie sono indicate nelle procedure e nei documenti del sistema di gestione della qualità aziendale.

3.4. Responsabilità

- **Tutto il personale** che a qualsiasi titolo collabora con l'azienda è responsabile dell'osservanza della presente policy ed è tenuto a partecipare alla segnalazione delle anomalie, anche formalmente non codificate, di cui dovesse venire a conoscenza.
- **Comitato di sicurezza delle informazioni** istituito per incontri pianificati semestralmente. Fanno parte di tale comitato la **Direzione**, il **Responsabile della sicurezza dei dati**, ed il **Responsabile dei sistemi di gestione.** Il compito di tale comitato è quello di fissare gli obiettivi, assicurare un indirizzamento chiaro con le strategie aziendale e promuovere un supporto evidente alle iniziative di sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza.
- **Responsabile della Sicurezza delle Informazioni** che si occupa della progettazione del sistema della Sicurezza delle Informazioni ed in particolare**:**
    - Suggerire le misure di sicurezza organizzative, procedurali, tecnologiche a tutela della sicurezza e per la continuità delle attività in e di **Ifin Sistemi**.
    - Controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce.
    - Verificare gli incidenti di sicurezza ed adottare le opportune contromisure.
- **Responsabile dei Sistemi di Gestione** che si occupa di**:**
    - Emanare tutte le norme necessarie ivi inclusa la classificazione e divulgazione dei documenti affinché l'organizzazione aziendale possa condurre in modo sicuro le proprie attività.
    - Pianificare per il personale un percorso formativo specifico e periodico in materia di sicurezza.
    - Promuovere la cultura relativa alla sicurezza delle informazioni.
    - Contribuire alla definizione delle contromisure da adottare a seguito di eventuali incidenti.
- **Tutti i soggetti esterni** che intrattengono rapporti con **Ifin Sistemi** devono garantire il rispetto dei requisiti della sicurezza esplicitati dalla presente politica di sicurezza anche tramite la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non è espressamente previsto nel contratto.

3.5. Applicabilità

La presente politica si applica indistintamente a tutti gli organi dell'azienda. L'attuazione della presente politica è obbligatoria per tutte le risorse di **Ifin Sistemi**, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda. **Ifin Sistemi** consente la comunicazione e diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che avvengono sempre nel rispetto delle regole nonché delle norme e leggi cogenti.

La Direzione