ZUCCHETTI Digital Solutions | Business Unit Ifin Sistemi

Politica per il Cloud

Rev.	Data	Redatto	Approvato	Note
01	26.02.2026	Legale Rappresentante Giovanni Maria Martingano	Direzione	A seguito della fusione per incorporazione di Ifin Sistemi S.r.l. in Zucchetti Digital Solutions S.r.l., avvenuta in data 01/01/2026, il presente documento è stato riesaminato e riallineato alla nuova configurazione societaria. La numerazione delle revisioni è stata reimpostata a partire dalla presente versione.
02	29.09.2026	Legale Rappresentante Giovanni Maria Martingano	Direzione	Aggiornamento riferimenti ISO/IEC 27001 (cap. 1)

Sommario

1.MISSIONE 3

2.OBIETTIVI 3

3.POLITICA E OBIETTIVI DEL SISTEMA ISO/IEC 27017:2015 4

4.POLITICA E OBIETTIVI DEL SISTEMA ISO/IEC 27018:2019 5

5.IMPEGNO DELLA DIREZIONE 6

6.APPLICABILITA' 7

1. MISSIONE

A seguito della fusione per incorporazione di Ifin Sistemi S.r.l. in Zucchetti Digital Solutions S.r.l., avvenuta in data 01/01/2026, il presente documento è stato riesaminato e riallineato alla nuova configurazione societaria. In tale contesto, le attività precedentemente svolte da Ifin Sistemi sono oggi riferite a **Zucchetti Digital Solutions S.r.l. – Business Unit Ifin Sistemi** (d'ora in avanti anche "BU IFIN" o "Organizzazione").
L'organizzazione si propone come una realtà leader nel guidare i propri clienti verso l'implementazione di soluzioni paperless, mediante la fornitura di soluzioni ICT e di consulenza specialistica per:

- la gestione e conservazione a norma dei documenti informatici;
- l'emissione, la trasmissione, la ricezione e conservazione di fatture elettroniche;
- soluzioni trusted per attestare autenticità, integrità e valore legale dei documenti digitali;
- soluzioni per l'archiviazione documentale.

I nostri Clienti operano in ambito bancario, commerciale, industriale e nella Pubblica Amministrazione. Il nostro interesse è quello di acquisire la loro fiducia in qualità di fornitori e di mantenere ed ampliare la nostra posizione di leader nel mercato digitale.
BU IFIN si impegna a comprendere le necessità dei clienti e pianificare le proprie attività per soddisfarle completamente attraverso l'identificazione e valutazione delle loro aspettative e la loro trasformazione in requisiti definiti e misurabili. Allo stesso modo opera nel rispetto delle richieste e dei requisiti:

- del mercato di riferimento;
- dello Stato in cui opera, adempiendo a leggi e regolamenti;
- di tutte le parti interessate.

Tali obiettivi sono raggiungibili da BU IFIN realizzando un Sistema di Gestione Integrato conforme alla norma UNI EN ISO 9001:2015 "Sistema Gestione Qualità", alla norma ISO/IEC 27001:2022 "Sistema Gestione Sicurezza delle Informazioni", alla norma ISO/IEC 27017:2015 "Controlli per la sicurezza delle informazioni dei servizi cloud", alla norma ISO/IEC 27018:2019 "Codice di condotta sulla protezione dei dati personali nel cloud" e alla norma UNI ISO 37001:2016 "Sistemi di Gestione per la Prevenzione della Corruzione".
BU IFIN è inoltre presente sul Marketplace AgID dedicato ai Conservatori qualificati per la fornitura di servizi di conservazione per conto della Pubblica Amministrazione.

2. OBIETTIVI

Gli obiettivi etici principali di BU IFIN sono:

- mantenere nei riguardi dei colleghi un rapporto onesto e trasparente: l'Azienda è di tutti per 365 giorni l'anno e tutti collaborano spendendo le migliori energie al bene comune;
- avere sempre un rapporto di correttezza nei riguardi dei Clienti e dei Fornitori, che sono entrambi vissuti come Partner strategici;
- creare un'Azienda in cui l'aggiornamento tecnologico sia tale da evitare l'obsolescenza culturale ed anzi avere l'ambizione di utilizzare sempre le tecnologie più avanzate che il mercato informatico è in grado di mettere a disposizione.

In tale ottica, BU IFIN, riconoscendo l'importanza strategica delle risorse umane, dei dispositivi informatici e delle infrastrutture, nonché del patrimonio delle informazioni, ha deciso di tutelarne la salvaguardia in tutte le

fasi dei processi aziendali, considerando l'Information Security uno strumento che permette la condivisione sicura delle informazioni ed il miglioramento delle prestazioni rese ai Clienti e della propria immagine.
Gli obiettivi di BU IFIN sono quindi:

- certificazione del Sistema di Gestione della Sicurezza delle Informazioni con estensione ai controlli delle norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019 e mantenimento della stessa nel triennio successivo;
- rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il Rischio Residuo a livelli accettabili;
- definizione di reazioni idonee al manifestarsi di incidenti di sicurezza, per garantire la continuità dell'operatività in sicurezza (Business Continuity);
- riduzione delle vulnerabilità dei propri asset aziendali da minacce quali virus, software nocivo ecc., tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:
  - sistemi hardware e software (personal computer, workstation, server, supporti di memorizzazione, apparecchiature di rete, sistemi di comunicazione elettronica);
  - informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);
  - servizi (posta elettronica e accessi al portale).
- caratterizzazione della propria offerta di servizi ai Clienti con la garanzia della salvaguardia delle informazioni condivise mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in **BU IFIN** e/o definite in sede contrattuale.

3. POLITICA E OBIETTIVI DEL SISTEMA ISO/IEC 27017:2015

BU IFIN, al fine di proteggere le informazioni archiviate e gestite in Cloud, in conformità dello standard ISO/IEC 27017:2015, assicura i seguenti requisiti:

- definire le informazioni archiviate nell'ambiente del Cloud che sono gestite dal Provider del Cloud;
- gli asset mantenuti sul Cloud, come le applicazioni;
- i processi in multi-tenant che si possono svolgere nel Cloud virtuale;
- gli utenti del Cloud ed il contesto in cui essi utilizzano il servizio;
- gli amministratori del servizio Cloud che hanno un accesso privilegiato;
- la localizzazione geografica del Provider del Cloud ed i Paesi in cui quest'ultimo può archiviare i dati relativi al Cloud (anche temporaneamente);
- i requisiti base di sicurezza delle informazioni applicabili alla progettazione ed alla implementazione del servizio Cloud;
- i rischi derivanti da addetti ai lavori autorizzati;
- accesso agli asset da parte del Provider;
- procedure per il controllo accessi, come la strong authentication per l'accesso amministrativo al Cloud;
- comunicazioni con il Provider durante il change management;
- allineamento e sicurezza degli ambienti virtuale e Cloud;
- accesso ai dati e loro protezione;
- gestione del ciclo di vita dell'account;
- comunicazione di Data Breach e linee guida per la condivisione delle informazioni, per aiutare le investigazioni.

BU IFIN mette in pratica una Privacy Policy, descrivendo le modalità con cui tratta i Dati Personali nell'ambito del servizio di Cloud Computing, anche alla luce degli obblighi imposti dal Regolamento (UE) 2016/679.
BU IFIN assicura che vengano soddisfatte le seguenti condizioni:

- i dati archiviati sui server rimangono sempre di proprietà dell'Azienda;
- imporre adeguati controlli di accesso e garantire che i dati in transito e il caricamento o il trasferimento di file siano protetti con protocolli di crittografia;
- concedere la possibilità di scaricare una copia dei dati in qualsiasi momento ed in totale autonomia;
- monitorare periodicamente le prestazioni e il rispetto del contratto.

In tale ambito, il percorso definito dalla Direzione prevede:

- certificazione del Sistema di Gestione della Sicurezza delle Informazioni con estensione ai controlli delle norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019 e mantenimento della stessa nel triennio successivo;
- rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il Rischio Residuo a livelli accettabili;
- attuazione, ove necessario, di idonee Azioni Correttive per ridurre a livelli ritenuti accettabili l'incidenza di condizioni anomale sul funzionamento complessivo del sistema;
- definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (Business Continuity);
- stabilizzazione e progressivo miglioramento del livello di sicurezza, anche attraverso l'attuazione di idonee azioni preventive, rispetto agli indicatori misurati negli anni precedenti.

4. POLITICA E OBIETTIVI DEL SISTEMA ISO/IEC 27018:2019

Relativamente allo Standard ISO/IEC 27018:2019, BU IFIN garantisce l'implementazione dei controlli richiesti per il trattamento di Dati Personali implementando adeguate misure di protezione, nel rispetto dei seguenti requisiti:

- **scelta e Consenso:** monitorare che il Provider del Cloud consenta l'esercizio dei diritti di accesso, rettifica e/o cancellazione da parte dell'Interessato, attraverso le informazioni rilevanti e le misure tecniche specificate nel contratto;
- **finalità del trattamento**: le finalità del trattamento sono rese note nel contratto di servizio con il Provider del Cloud;
- **minimizzazione dei dati**: file e documenti temporanei devono essere cancellati o distrutti entro un periodo specificato e documentato;
- **limitazione all'uso, alla conservazione e alla divulgazione**: garantire che non avvenga la divulgazione di Dati Personali a Terze Parti. La richiesta di divulgazione di Dati Personali da parte di autorità amministrative o giudiziarie è notificata dal Provider in maniera tempestiva;
- **trasparenza**: in caso di ricorso a subappaltatori da parte del Provider è reso noto prima del loro utilizzo. Le disposizioni per l'utilizzo dei subappaltatori sono riportate in chiaro nel contratto con il Provider. Quest'ultimo informa BU IFIN in modo tempestivo di eventuali modifiche previste in questo senso, in modo tale da concedergli la possibilità di opporsi a tali modifiche o di risolvere il contratto;
- **accountability**: in caso di violazioni che comportano perdite, diffusione o modifica dei Dati Personali (Data Breach), il Provider effettua la notifica tempestivamente attraverso un processo interno di Incident Management;

- **conformità alla privacy**: il Provider indica i Paesi in cui sono conservati i dati, anche derivanti dall'utilizzo di subappaltatori e indica specifici accordi contrattuali applicati in merito al trasferimento internazionale di dati. Il Provider informa tempestivamente BU IFIN di eventuali modifiche previste a tale riguardo, in modo da concedergli la possibilità di opporsi o di recedere dal contratto.

Inoltre, le seguenti azioni sono assicurate dal Provider nel senso più esteso dei controlli Cloud:

- fornire procedure di accesso sicuro per qualsiasi account richiesto per gli utenti sotto il controllo di BU IFIN;
- fornire le informazioni in merito alle circostanze in cui si utilizza la crittografia per proteggere le informazioni personali che vengono elaborate;
- effettuare smaltimento o riutilizzo sicuro delle apparecchiature contenenti supporti di memorizzazione;
- effettuare la valutazione del rischio e attuare misure tecniche e organizzative per ridurre al minimo i rischi identificati, anche tramite Accordi di Riservatezza o di Non Divulgazione tra il Provider e i suoi Dipendenti e Collaboratori;
- implementare meccanismi per il backup off-site per la protezione dalla perdita di dati, garantendo continuità alle operazioni di trattamento dei dati e fornendo la possibilità di ripristinare le operazioni di trattamento dei dati dopo un evento dirompente;
- limitare la creazione di materiale cartaceo (comprese le stampe che contengono dati personali);
- attuare procedure di controllo e registrazione per il ripristino dei dati;
- attuare una procedura di autorizzazione per i Dati Personali trasferiti su supporti magnetici al di fuori dei locali aziendali del Provider e crittografia dei contenuti;
- vietare l'utilizzo di supporti e dispositivi di memorizzazione portatili non crittografati a meno di eccezioni;
- crittografare i dati che vengono trasmessi sulle reti pubbliche;
- consentire lo smaltimento sicuro dei materiali cartacei;
- utilizzare ID univoci per i Clienti Cloud;
- consentire stesura e aggiornamento sistematico di un registro degli utenti che accedono al sistema e dei relativi profili di accesso;
- gestire gli ID utente e vietare l'assegnazione ad altri di quelli non utilizzati o scaduti;
- fornire evidenza dei controlli minimi di sicurezza nei contratti con i subappaltatori;
- fornire la garanzia che ogni volta che lo spazio di archiviazione dei dati viene assegnato a un nuovo Cliente del servizio Cloud, tutti i dati che precedentemente risiedevano su tale spazio di archiviazione siano stati resi intellegibili;
- raggiungere la conformità rispetto alle condizioni contrattuali concordate.

5. IMPEGNO DELLA DIREZIONE

Il Sistema di Gestione identifica e tiene conto dei requisiti derivanti dall'evoluzione del contesto interno ed esterno, in particolare dei requisiti delle terze parti interessate e identifica gli obiettivi di sicurezza da perseguire. L'Alta Direzione si impegna ad allocare le risorse necessarie alla realizzazione del predetto sistema e mantiene un "commitment" adeguato sulle tematiche della sicurezza, assicurando che gli obiettivi di sicurezza siano integrati nei processi aziendali e conseguiti.

6. APPLICABILITA’

In considerazione dell'importanza degli obiettivi da raggiungere e dell'impegno necessario per il loro ottenimento, si invita tutto lo Staff a prestare la propria disponibilità e collaborazione nell’attuazione ed aggiornamento del Sistema e ad attenersi scrupolosamente alle prescrizioni contenute nel Manuale di Gestione della Sicurezza delle Informazioni, nelle Procedure Operative e nelle altre disposizioni in merito eventualmente fornite dal Management.

La Direzione di Zucchetti Digital Solutions - BU IFIN