Politica per la sicurezza delle informazioni

Rev. 01 del 08/09/2021

INDICE

SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da SATIP S.r.l. al fine di sviluppare un efficace e sicuro Sistema di Gestione della Sicurezza delle Informazioni (di seguito SGSI).

IL CONTESTO

SATIP è un operatore del document management. SATIP archivia e digitalizza documentazione per conto dei clienti, gestendola nel rispetto delle più stringenti normative nazionali e europee.

Per SATIP la sicurezza delle informazioni è fattore irrinunciabile per la protezione del proprio patrimonio informativo e quello dei propri Clienti ed è per questo che all'interno dell'azienda viene posta particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione, sviluppo erogazione e manutenzione dei propri servizi, ritenuti bene primario dell'azienda.

Consapevole del fatto che la gestione dei servizi per i Clienti possa comportare l'affidamento di dati e informazioni critiche, SATIP opera secondo normative di sicurezza riconosciute in ambito internazionale. SATIP intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio la riservatezza, l'integrità e la disponibilità sia del patrimonio informativo interno che di quello che è stato ad essa affidato dai propri Clienti.

Su tali basi SATIP ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità ai requisiti della norma internazionale UNI EN ISO/IEC 27001.

DESTINATARI

La politica per la sicurezza delle informazioni di SATIP deve essere conosciuta, ed i principi in essa contenuti rispettati integralmente, da tutto il personale interno, i collaboratori, i fornitori e tutte le terze parti che a vario titolo entrano in contatto con le informazioni protette dal SGSI di SATIP.

DISTRIBUZIONE

La presente politica è distribuita sul sito web ufficiale di SATIP (www.satipsrl.it), che ne mette a disposizione la versione approvata più aggiornata. Qualunque copia di questo documento non sia appena stata scaricata dal sito aziendale è da considerarsi non aggiornata. Di conseguenza, è responsabilità del lettore assicurarsi di ottenere la versione più aggiornata ed attuale del documento.

DOCUMENTI APPLICABILI E RIFERIMENTI NORMATIVI

Norme di legge

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- D.lgs. 231/2001, art.24-bis “Delitti informatici e trattamento illecito di dati”;
- D.lgs. 169/99 “Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati”;
- D.lgs. 259/2003 “Codice delle comunicazioni elettroniche”;
- D.lgs. 196/2003 “Codice in materia di protezione dei dati personali”;
- Provvedimento del Garante per la Protezione dei Dati Personali “Misure di sicurezza obbligatorie per le intercettazioni” (Provvedimento del 15 settembre 2005);
- Provvedimento del Garante per la Protezione dei Dati Personali “Misure e disposizioni volte a salvaguardare gli interessati in relazione alla conservazione dei dati relativi al traffico telefonico e Internet per l'individuazione e la soppressione dei reati” (Provvedimento del 17 gennaio 2008);
- Provvedimento del Garante per la Protezione dei Dati Personali “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle

attribuzioni delle funzioni di amministratore di Sistema" (Provvedimento del 27 novembre 2008);

- Legge 22 aprile 1941, n.633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
- Provvedimento del Garante per la Protezione dei Dati "Misure concernenti la videosorveglianza" (Provvedimento del 8 aprile 2010);
- Legge 23 dicembre 547/93 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
- Legge 18 marzo 48/2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" (Convenzione di Budapest).

Standard di riferimento

- ISO/IEC 27001 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti";
- ISO/IEC 27000 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni – Overview e vocabolario".

Documenti aziendali

La documentazione aziendale di riferimento viene fornita su richiesta e in linea con il livello di confidenzialità del documento richiesto.

QUADRO DI RIFERIMENTO PER LA DEFINIZIONE DEGLI OBIETTIVI DI SICUREZZA

Gli obiettivi di sicurezza delle informazioni di SATIP vengono definiti in relazione agli obiettivi strategici e di business ed a loro sostegno, nel rispetto degli impegni contrattuali e delle normative vigenti nelle giurisdizioni di riferimento. Il raggiungimento di tali obiettivi di sicurezza viene pianificato, attuato, monitorato e controllato con il supporto una specifica metodologia di gestione del rischio. Gli obiettivi di sicurezza ed il grado di conseguimento degli stessi, vengono riesaminati almeno una volta l'anno.

CONTENUTO DELLA POLITICA

Il Sistema di Gestione per la Sicurezza delle Informazioni di SATIP definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- Riservatezza: l'informazione deve essere nota solo a chi dispone di opportuni privilegi;
- Integrità: l'informazione deve essere modificabile solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità: l'informazione deve essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi.

Questa politica definisce i principi di sicurezza delle informazioni che guidano:

- I comportamenti dei soggetti cui essa è indirizzata, nell'ambito del SGSI;
- L'implementazione di processi, procedure, istruzioni, l'adozione di pratiche ed altri controlli nell'ambito del SGSI.

Di seguito sono espressi i principi che determinano e sostengono la definizione ed attuazione del SGSI a garanzia della sicurezza delle informazioni.

Principio 1

Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione di servizi e ai dati ad esse collegati, alla tutela dei prodotti e alla relativa gestione delle piattaforme e applicazioni di document management.

Principio 2

Tutte le informazioni essenziali ai servizi (ad es. documenti tecnici e commerciali, informazioni di configurazione, e-mail relative al servizio, informazioni fornite dai clienti della piattaforma, ecc.) devono essere protette.

Principio 3

Tutte le informazioni da proteggere devono essere gestite secondo il livello di classificazione attribuito, nel rispetto delle relative procedure, lungo tutto il loro ciclo di vita.

Principio 4

La sicurezza delle informazioni costituisce un aspetto fondamentale per il conseguimento degli obiettivi di business. Il conseguimento ed il mantenimento della certificazione ISO 27001 costituiscono una prova tangibile, visibile e valutabile da terze parti, in relazione all'impegno di SATIP nella garanzia della sicurezza delle informazioni. La perdita o sospensione di tale certificazione è ritenuta un grave danno di immagine ed un potenziale rischio per il conseguimento degli obiettivi di business.

Principio 5

Tutti coloro i quali entrano a vario titolo in contatto con le informazioni da proteggere hanno un ruolo diretto nel successo di tale protezione. È dunque responsabilità diretta ed esplicita di tali soggetti attenersi ai principi contenuti nella presente politica ed in tutte le politiche di sicurezza applicabili ad essa correlate e garantirne il rispetto.

Principio 6

La sicurezza delle informazioni viene progettata ed attuata in modo da essere parte integrante dei normali processi e comportamenti di business e definita in modo da non pregiudicare l'adeguatezza degli stessi ai fini ed agli scopi dell'organizzazione.

Principio 7

Il conseguimento degli obiettivi di sicurezza viene governato mediante un approccio basato sul rischio, che prevede l'applicazione di un processo di gestione del rischio che tiene in considerazione il contesto dell'organizzazione, il campo di applicazione del SGSI, gli obiettivi dell'organizzazione.

Principio 8

L'organizzazione adotta un processo strutturato per la gestione degli incidenti di sicurezza delle informazioni mirato a contenerne gli impatti, ad individuarne le cause ed a favorirne la rimozione. Tutti i soggetti interessati dal SGSI sono tenuti alla segnalazione di circostanze anomale o sospette riguardo alle informazioni.

RESPONSABILITÀ

Il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni si occupa della progettazione del SGSI ed in particolare di:

- Emanare tutte le norme necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- Adottare criteri e metodologie per l'analisi e la gestione del rischio;
- Suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di SATIP;
- Pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;
- Controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- Verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- Promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni che intrattengono rapporti con SATIP S.p.A. devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

RIESAME

SATIP S.p.A. verificherà periodicamente, con cadenza almeno annuale, o più frequente in caso di cambiamenti significativi per quanto concerne la sicurezza delle informazioni, l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni e la presente politica, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.