ENTAKSISOLUTIONS

SISTEMA DI GESTIONE CERTIFICATO
ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
SERVIZI FIDUCIARI QUALIFICATI
ETSI 319 401 | ETSI 319 411-1 e 2 | ETSI 319 421 | ETSI 119 511
FIRME E SIGILLI ELETTRONICI - MARCHE TEMPORALI
CONSERVAZIONE A LUNGO TERMINE

Manuale

MAN SIG 20200511 Politica per la sicurezza delle informazioni

Entaksi Solutions SpA

Firma digitale apposta da: Alessandro Geri
In data: 11/04/2024 06:53:56
Motivo: Firma Approvazione Amministratore Unico
Campo: FirmaAmmUnico
223be001-bce8-46ea-8ce9-0259a93268d7

Indice

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manuale
Nome documento	MAN SIG 20200511 Politica per la sicurezza delle informazioni
Versione	1.3.0
Data creazione	11/05/2020
Ultima revisione	06/12/2023
Autore	Alessia Soccio
Stato	Rilasciato
Classificazione	Pubblico

Riproduzioni cartacee di questo documento sono da considerarsi copie di lavoro non censite dal SIG.

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
11/05/2020	0.0.1	Alessia Soccio	RARC	Creazione bozza - da precedente IO ISO 20170621 Disposizione sulla sicurezza delle informazioni.	Interno
25/11/2020	1.0.0	Alessia Soccio	RARC	Revisione e rilascio.	Pubblico
01/12/2021	1.1.0	Alessia Soccio	RSIG	Aggiornamento policy progettazione e modifica forma giuridica da Srl a SpA.	Pubblico
10/05/2023	1.2.0	Alessia Soccio	RSIG	Aggiornata descrizione certificazioni e standard di riferimento, aggiornato documento per implementazione Sistema di Gestione dei Servizi Fiduciari e Sistema di Gestione della Prevenzione della Corruzione.	Pubblico
06/12/2023	1.3.0	Alessia Soccio	RSIG	Aggiornata per ampliamento Sistema di Gestione dei Servizi Fiduciari.	Pubblico

Approvazione del documento

Data	Addetto	Mansione	Firma
06/12/2023	Alessandro Geri	Amministratore Unico	*Firmato digitalmente*

© 2023 Entaksi Solutions SpA.

Le informazioni contenute nel presente documento sono di proprietà di Entaksi Solutions SpA, sono fornite ai destinatari in via riservata e confidenziale e non possono essere usate per fini produttivi, né comunicate a terzi o riprodotte, per intero o in parte, senza il consenso scritto di Entaksi.

1. Introduzione

1.1. Obiettivi del documento

Il presente documento contiene la descrizione delle politiche adottate da Entaksi Solutions SpA riguardo la sicurezza delle informazioni, e corrisponde a quello che viene anche chiamato *Information Security Policy Document* (ISPD).

La gestione della sicurezza delle informazioni è parte centrale e fondamentale delle attività di Entaksi, in quanto l'azienda ha scelto di agire come Qualified Trust Service Provider all'interno dell'Unione europea, in conformità con il Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio - eIDAS.

L'obiettivo principale di questa politica è documentare tutte le strategie e gli accorgimenti procedurali attraverso i quali Entaksi si propone di tutelare le informazioni documentate presenti a qualunque titolo nel proprio sistema informativo.

La finalità generale è quella di garantire un adeguato livello di protezione dei dati, che comprendono sia quelli dell'azienda che quelli conservati e gestiti per clienti e terze parti.
Il presente documento espone il progetto di sicurezza e i suoi obiettivi come definiti nel SIG adottato dall'azienda, basato su standard internazionali di riferimento in materia e alle disposizioni legislative vigenti in materia di sicurezza, privacy e trattamento dei dati.

1.2. Campo di applicazione

La presente disposizione si applica ad ogni Utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza della Società.

La presente disposizione è pubblica, in quanto i principi in essa contenuti riguardano anche aspetti relativi ai servizi erogati da Entaksi, e pertanto si ritiene opportuno che gli utenti che utilizzano tali servizi siano messi a conoscenza di tutte le azioni e le procedure interne intraprese da Entaksi a salvaguardia delle informazioni raccolte o conservate dalla Società.

1.3. Definizioni e documentazione di riferimento

Per *Utente* si intende a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per *Società* si intende, invece, la società Entaksi Solutions SpA, la quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

2. Politiche per la sicurezza delle informazioni

Nel proprio processo di revisione e di miglioramento dei processi Entaksi Solutions SpA ha deciso di intraprendere il percorso di istituzione di un Sistema Integrato di Gestione (SIG) che copra interamente le attività caratteristiche della Società, nel rispetto della sicurezza delle informazioni.

Il SIG comprende progettazione, produzione, commercializzazione, installazione e assistenza di applicativi software, erogazione di servizi informatici quali ad esempio la distribuzione in modalità SaaS (Software as a Service) degli applicativi.

Il SIG di cui si è dotata Entaksi Solutions SpA è il risultato della adozione coordinata e integrata di sistemi di gestione conformi alle norme:

- **ISO 9001:2015 - Sistema di Gestione Qualità (SGQ)**
- **ISO/IEC 20000-1:2018 - Sistema di Gestione della erogazione dei servizi IT (SGS)**
- **ISO/IEC 27001:2013 - Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27017:2015 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27018:2019 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27035:2016 - Sistema di Gestione degli Incidenti di Sicurezza delle Informazioni (SiGI)**
- **ISO/IEC 22301:2019 - Sistema di Gestione della Continuità Operativa Aziendale (BCMS)**
- **UNI ISO 37001:2016 - Sistema di Gestione della Prevenzione della Corruzione (SGPC)**
- **Sistema di Gestione dei Servizi Fiduciari (SGSF)**:
  - **ETSI EN 319 401**
  - **ETSI EN 319 411-1**
  - **ETSI EN 319 411-2**
  - **ETSI EN 319 412-1,2,3,5**
  - **ETSI EN 319 421**
  - **ETSI TS 119 511**

L'obiettivo generale della Società è la gestione corretta di tutte le informazioni generate o trattate al fine di garantire la continuità gestionale e prevenire o minimizzare i danni gestionali, con specifica attenzione alle particolari modalità organizzative ed operative che la Società ha deciso di adottare (outsourcing infrastrutture centrali di elaborazione, ricorso strutturale al telelavoro). Inoltre in alcuni ambiti specifici che fanno parte del core business della Società, quali la Conservazione Documentale a norma di legge, sostitutiva o nativa, di documenti informatici, gli standard di riferimento contemplano anche la caratteristica di **non ripudiabilità** del dato, ottenuta mediante apposizione della firma digitale o qualificata.

La Direzione ritiene che la salvaguardia della riservatezza, integrità, disponibilità e, ove reso necessario dal contesto applicativo, della non ripudiabilità delle informazioni siano aspetti fondamentali per assicurare, oltre la conformità legale, il mantenimento di una affidabile immagine di impresa verso i propri dipendenti, collaboratori, clienti, fornitori e terze parti interessate.

La Direzione è consapevole che la corretta gestione della sicurezza delle informazioni riguarda tutti gli aspetti della vita societaria, ed è quindi attivamente impegnata ad ottenere la partecipazione competente e responsabile di tutti i collaboratori di Entaksi Solutions e, per quanto possibile, dei Soggetti Terzi interessati.

2.1. Politica per la protezione dei dati personali

Entaksi fornisce ai propri dipendenti, collaboratori, fornitori o consulenti, istruzioni organizzative e tecniche che consentano l'osservanza degli obblighi di legge relativi alla protezione dei dati personali. Per questi obblighi delinea il quadro di sicurezza adottato per il sistema informativa, e definisce tutte le misure per garantire l'affidabilità delle componenti hardware e software ai fini della tutela dei dati personali trattati.
Inoltre provvede a informare gli utenti di prodotti e servizi delle misure messe in atto per proteggere e conservare i dati personali attraverso le apposite informative.

3. Organizzazione della sicurezza delle informazioni

3.1. Organizzazione interna

Vengono di seguito riportati i ruoli assunti all'interno di Entaksi per quanto riguarda la sicurezza delle informazioni.

Tabella 1. Ruoli all'interno dell'organizzazione rispetto alla sicurezza delle informazioni.

Ruolo	Responsabilità
Amministratore Unico	Pianifica, controlla e supervisiona le attività della Società. Formula la Politica della Società e i relativi indirizzi strategici, inclusi quelli riguardanti la sicurezza delle informazioni.
Direzione / Rappresentante della Direzione	Definisce e verifica le informazioni documentate da produrre, e garantisce la loro rintracciabilità e conservazione. Pianifica, coordina e supervisiona le attività aziendali di concerto con l'Amministratore Unico.
Responsabile del Sistema Integrato di Gestione (SIG)	Mantiene aggiornato il SIG, e ne gestisce la documentazione, verifica la conformità, l'efficacia e l'efficienza del SIG.
Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (SiGSI)	Ha la responsabilità di tutte le attività inerenti la sicurezza delle informazioni del sistema informativo di produzione.
Responsabile Tecnico (RICT)	Ha la responsabilità di assicurare la pianificazione dell'architettura, lo sviluppo e la gestione dei sistemi di Information Technology della Società, garantendo l'integrazione delle piattaforme hardware/software, la coerenza dei sistemi/processi e l'uniformità della diffusione sul territorio.
Responsabile dell'Incident Response Team (IRT)	Coordina l'Incident Response Team e ha la responsabilità della gestione degli incidenti che coinvolgono la sicurezza delle informazioni.
Responsabile del Servizio di Conservazione (ReCON)	È il soggetto responsabile della creazione e del mantenimento del sistema e del processo di conservazione documentaria. Definisce e attua le politiche complessive del Sistema di Conservazione, e ne governa la gestione.
Funzione di Conformità per la prevenzione della corruzione (FDC)	All'interno dell'organizzazione è destinataria delle segnalazioni relative a possibili fenomeni corruttivi e ne garantisce la riservatezza e il corretto trattamento.
Security Officer	Nell'ambito dell'amministrazione del Sistema di Gestione dei Servizi Fiduciari si occupa di garantire la sicurezza di questi ultimi, e l'amministrazione delle pratiche di sicurezza derivanti dal Regolamento UE no. 910/2014 - eIDAS.

4. Classificazione delle informazioni

Le informazioni possono essere classificate come:

- Riservate.
- Confidenziali.
- Pubbliche.

Questa classificazione deriva dalla tipologia delle informazioni (fondamentali o di supporto) e dal pubblico che può avere accesso alle suddette informazioni (ristretto, interno, circoscritto o allargato), secondo il seguente schema:

	Ristretto	**Interno**	**Circoscritto**	**Allargato**
Fondamentale	Riservato	Riservato	Confidenziale	Pubblico
Di supporto	Riservato	Confidenziale	Confidenziale	Pubblico

I documenti che veicolano le informazioni sono di conseguenza così classificati:

- **Informazioni fondamentali riservate (uso ristretto o interno)**: dati sensibili che non sono oggetto di divulgazione al di fuori di un ristretto insieme di addetti.
  I documenti che contengono questo tipo di informazioni sono classificati come “Riservati”.
- **Informazioni fondamentali confidenziali (uso circoscritto)**: dati che non sono oggetto di divulgazione al pubblico.
  I documenti che contengono questo tipo di informazioni sono classificati come “Confidenziali”.
- **Informazioni fondamentali non confidenziali (uso pubblico)**: dati oggetto di divulgazione al pubblico, senza alcun requisito di riservatezza.
  I documenti che contengono questo tipo di informazioni sono classificati come “Pubblici”.
- **Informazioni di supporto riservate (uso interno)**: dati che non sono oggetto di divulgazione al di fuori di un ristretto insieme di addetti.
  I documenti che contengono questo tipo di informazioni sono classificati come “Riservati”.
- **Informazioni di supporto confidenziali (uso interno o circoscritto)**: documenti / informazioni specificatamente legate al Sistema e al suo funzionamento la cui divulgazione a soggetti non autorizzati potrebbe compromettere l’efficacia delle contromisure poste in essere nel Sistema Integrato di Gestione a protezione della disponibilità, integrità e riservatezza delle informazioni.
  I documenti che contengono questo tipo di informazioni sono classificati come “Confidenziali”.
- **Informazioni di supporto non confidenziali (uso pubblico)**: documenti / informazioni specificatamente legate al Sistema e al suo funzionamento la cui divulgazione non compromette in alcun modo l’efficacia delle procedure poste in essere nel Sistema Integrato di Gestione.
  I documenti che contengono questo tipo di informazioni sono classificati come “Pubblici”.

Tutte le informazioni derivate da contatti con i clienti, compresi i documenti portati in conservazione e i dati personali delle registrazioni ai servizi, sono considerate informazioni fondamentali, accessibili solo a un pubblico ristretto, e sono pertanto classificate come riservate.

Le informazioni riguardanti gli utenti dei servizi Entaksi pertanto non sono assolutamente oggetto di divulgazione al di fuori degli addetti al servizio stesso, e sono soggette a cifratura.

Tutte le informazioni devono essere classificate secondo un livello adeguato che ne definisca il grado di riservatezza, integrità e disponibilità.

Riservatezza	L’accesso ai dati deve essere limitato in base ai privilegi indicati per gli utenti definiti, in accordo con il loro livello di classificazione. Le informazioni devono essere protette da eventuali accessi non autorizzati.
Integrità	Le informazioni devono essere complete e precise. Tutti i sistemi, gli asset e le reti devono funzionare correttamente, secondo specifiche che ne garantiscano la piena operatività.
Disponibilità	Le informazioni devono essere disponibili all’accesso e poter essere distribuite a chi ne detiene i diritti in base al livello di classificazione.

Tutto il personale di Entaksi interessato nella creazione o nella gestione delle informazioni deve assicurare che le stesse siano classificate, e che vengano trattate in accordo al livello di classificazione scelto.

Viene definito per il sistema di conservazione il ruolo di “Produttore”, ossia la persona fisica o giuridica responsabile della creazione del Pacchetto di Versamento (PDV) e del suo invio verso il sistema di conservazione.

I produttori dei documenti sono considerati un pubblico ristretto, e le informazioni versate nel sistema come "fondamentali".

Per questo motivo tutti i dati provenienti dai produttori inseriti nel sistema di conservazione sono considerati come "Informazioni riservate", e non sono oggetto di divulgazione al di fuori del rapporto tra i produttori e i responsabili individuati per il sistema di conservazione.

I principi indicati da Entaksi per garantire riservatezza, integrità e disponibilità delle informazioni sono i seguenti:

- Ogni utente che venga in possesso di informazioni riservate di Entaksi è considerato responsabile della protezione delle stesse, soprattutto dall’accesso di terzi e dall’uso non autorizzato.
- Tutti gli utenti hanno la responsabilità di proteggere le loro password aziendali e altre credenziali di accesso collegate ad attività aziendali da un uso non autorizzato.
- Tutti gli accessi e l’utilizzo di informazioni riservate di proprietà di Entaksi devono essere autorizzate da Entaksi, per gli scopi connessi all’attività aziendale.
- I dipendenti Entaksi e chiunque si trovi ad accedere a informazioni riservate di proprietà di Entaksi dovranno ricevere una adeguata formazione volta all’addestramento alla protezione delle stesse.
- Tutti gli utenti che utilizzano informazioni riservate appartenenti ad Entaksi devono essere univocamente identificati.
- Le informazioni riservate devono essere protette su qualsiasi dispositivo aziendale.
- Le informazioni riservate devono essere protette anche nel caso l’utente le trasferisca su un dispositivo non aziendale. In tal caso il dispositivo dovrà seguire le regole per i dispositivi aziendali (es.: cellulare personale connesso alla email aziendale).
- Tutti i server che memorizzano informazioni riservate appartenenti a Entaksi devono essere protetti da accessi non autorizzati.
- Tutti i dispositivi aziendali devono essere adeguatamente censiti e devono esserne note le loro ubicazioni fisiche abituali. Nel caso si verifichino spostamenti devono essere seguite le regole per il trasporto.
- I software vanno mantenuti aggiornati su tutti i dispositivi, in modo tale da garantire che le versioni correnti siano le più sicure. Le eventuali patch sono approvate dal Responsabile Tecnico, che provvede ad informare i dipendenti tramite i canali di comunicazione concordati che è possibile aggiornare i dispositivi in sicurezza.

Ogni violazione rispetto alle direttive contenute in questa disposizione deve essere riportata e trasmessa a tutti gli utenti interessati.

5. Controllo degli accessi

Entaksi garantisce la protezione delle credenziali attraverso l'utilizzo del protocollo OAuth 2.0 e gestisce le credenziali single sign-on attraverso il software Open Source Keycloak. Per la gestione delle credenziali di accesso Entaksi utilizza un sistema di gestione delle identità compatibile con gli standard OAuth2 (RFC-6749, RFC-6750, RFC-6819, RFC-7662, RFC-7009, RFC-7519), SAMLv2 e con il protocollo OpenID Connect.

Il sistema è implementato dal software open source *Keycloak*.

5.1. Dispositivi portatili e telelavoro

Entaksi Solutions ha deciso di utilizzare al massimo le opportunità tecnico-organizzative e normative offerte dallo stato attuale della tecnologia delle telecomunicazioni e dall'ordinamento legislativo in vigore, scegliendo di operare strutturalmente ed esclusivamente in modalità smart-working.

Per questo motivo non utilizza uffici fisici, ma piuttosto location di co-working.

Entaksi Solutions ha deciso di inquadrare in un rapporto di telelavoro tutti i dipendenti e collaboratori.

Il risultato diretto dell'adozione di questa impostazione è che la società opera totalmente in rete, senza una vera e propria sede operativa centrale.

5.2. Requisiti di business per il controllo degli accessi

L'aspetto della gestione della sicurezza delle informazioni riguardante la sicurezza logica e fisica ha come obiettivo l'adozione di un insieme di accorgimenti di natura tecnica, organizzativa e procedurale che, posti in essere in maniera sistematica, sono rivolti a governare e proteggere le informazioni del patrimonio informativo aziendale da tentativi di accesso logico non autorizzato.

Per quanto riguarda specificamente l'accesso ai sistemi, i requisiti di sicurezza si traducono nella adozione ed adeguata parametrizzazione e gestione di strumenti che consentano l'accessibilità alle informazioni alle sole persone autorizzate in ragione del loro ruolo e responsabilità, e, implicitamente, nella loro protezione contro minacce all'integrità, riservatezza e disponibilità delle stesse.

Nello specifico i requisiti per la sicurezza logica devono essere nel contesto operativo di Entaksi Solutions come particolarmente stringenti; infatti, bisogna tenere conto che, data l'organizzazione di Entaksi, centrata sul telelavoro e sul ricorso strutturale all'outsourcing delle risorse hardware e software condivise, il controllo dell'accesso fisico da parte di personale non autorizzato a queste infrastrutture non può essere totalmente sotto il controllo dalle procedure di Entaksi. Sebbene venga applicata una politica di qualifica del fornitore volta a ricercare particolari garanzie di sicurezza, quale ad esempio il possesso della certificazione ISO 27001, non è spesso possibile ottenere contrattualmente condizioni di imposizione di particolari controlli, dal momento che spesso il ricorso a aziende di grandi dimensioni non permette di ottenere condizioni contrattualmente vincolanti sul controllo della sicurezza fisica delle infrastrutture.

Perciò, benché in generale i servizi in outsourcing siano ragionevolmente presidiati e protetti, nella valutazione dei rischi collegati viene assegnata al massimo livello la probabilità di accadimento minimizzando l'impatto derivato dalle minacce correlate all'accesso fisico di persone non autorizzate ai locali e alle apparecchiature - e viene di conseguenza accettato il rischio del danno economico alle stesse in caso di atti vandalici, furti o manomissione dei sistemi - purché venga salvaguardata la sicurezza del dato.

Tale politica generale si traduce in particolari contromisure per il trattamento delle "Aree isolate", ossia quelle in cui sono presenti apparecchiature che devono risiedere all'interno di un perimetro fisico ben definito, isolato e protetto, al quale l'accesso è precluso ad altre organizzazioni ed è soggetto a controllo e registrazione dei passaggi. Dal momento che vengono richiesti particolari controlli di sicurezza per i dispositivi contenuti in tale perimetro, e che il danno economico e di reputazione derivante dal loro danneggiamento o manomissione è più elevato rispetto ad altre apparecchiature, vengono effettuati ulteriori controlli sul fornitore, che deve essere in grado di garantire requisiti di sicurezza più stringenti.

5.3. Gestione degli accessi degli utenti

Tutti gli utenti che accedono ai sistemi, sia quelli SIG che quelli afferenti ai servizi, sono profilati secondo un determinato gruppo, in modo da tutelare la segregazione dei ruoli e delle informazioni.

Ai servizi forniti da Entaksi viene applicata una gestione degli accessi che prevede la creazione di differenti comunità di utenti,

i cui privilegi di accesso sono assegnati in base alla logica RBAC (Role Based Access Control). I privilegi vengono assegnati in base a dei ruoli, e creati in base alle funzioni eseguibili nel servizio. I permessi per eseguire specifiche operazioni sono assegnate non per singolo utente ma in base a specifici ruoli.

I privilegi e i ruoli ad essi connessi vengono definiti nei documenti delle specifiche tecniche di ogni servizio.

Per ogni servizio sono presenti i seguenti ruoli:

- amministratore: utenti con accesso alle configurazioni del sistema.
- utenti: fruitori del sistema, che non hanno accesso alle configurazioni del sistema.
- auditor: utenti con accesso in sola lettura.

La definizione dei privilegi per ogni gruppo, dei ruoli, la gestione delle richieste di credenziali, delle loro revoche e dei tempi necessari alle stesse, sono gestite dal Responsabile dei Servizi, e la loro eventuale revisione avviene in accordo con il Responsabile Tecnico.

Il Responsabile Tecnico si occupa della procedura di registrazione dei dati di accesso in un apposito registro, e della sua integrità.

Mentre il sistema di gestione delle identità e il servizio Single Sign-On si occupano di garantire l'autenticazione dell'utente, il livello di autorizzazione, ovvero il ruolo dell'utente, è stabilito nel singolo componente applicativo.
Questo garantisce la separazione dei ruoli applicativi e una gestione dettagliata del livello di accesso alle singole applicazioni evitando la presenza di ruoli "super amministratori" che ereditano automaticamente accesso ad ogni livello dei servizi.

5.4. Responsabilità dell'utente

L'utente del sistema ha la responsabilità:

- degli accessi all'area protetta;
- della sicurezza delle apparecchiature affidate per il normale svolgimento delle attività;
- della comunicazione tempestiva alle autorità ed al Responsabile dell'Incident Response Team (IRT) di eventuali incidenti occorsi.

5.5. Controllo degli accessi ai sistemi e alle applicazioni

Il sistema SiGSI che controlla gli accessi al patrimonio informativo del sistema è in grado, anche con l'ausilio di strumenti specifici, di:

- controllare l'identità degli utenti che accedono al sistema;
- registrare tutti gli accessi autorizzati;
- segnalare i tentativi di accesso;
- registrare le attività svolte dall'utente sul sistema.

6. Crittografia

Entaksi Solutions SpA implementa una serie di tecniche basate su algoritmi di crittografia per l'archiviazione sicura delle informazioni, per la protezione delle informazioni quando vengono scambiate tra diversi sistemi e, in alcuni contesti, per l'autenticazione degli utenti e dei servizi. Tali tecniche si basano sull'implementazione della norma ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI) - Cryptographic Suites".

La gestione della crittografia si divide nelle seguenti aree:

- Gestione dei certificati TLS.
- Gestione delle chiavi SSH.
- Gestione delle chiavi GPG/PGP.
- Gestione delle password per la cifratura simmetrica delle informazioni.
- Gestione della crittografia per le firme digitali.

Entaksi utilizza il protocollo Transport Layer Security (TLS) versione 1.2 o superiore per le comunicazioni cifrate con i servizi esposti dall'infrastruttura sulla rete pubblica. Le precedenti versioni e i protocolli Secure Socket Layer (SSL) sono deprecati.

Gli ambiti di applicazione di questo protocollo sono:

1. Protezione delle connessioni ai servizi veicolati tramite protocollo HTTP.
2. Protezione delle connessioni ai servizi di posta elettronica o altri servizi basati su connessioni TCP.
3. Protezione delle connessioni VPN.
4. Protezione di altri canali di interconnessione tra servizi interni all'infrastruttura basati su TLS.

L'accesso ai sistemi GNU/Linux e ad una serie di servizi da questi gestiti avviene tramite protocollo SSH.

La complessità e gli algoritmi utilizzati per le chiavi crittografiche SSH sono fattori che dipendono dallo stato dell'arte dei prodotti software utilizzati per gestire l'accesso nonché dalle vulnerabilità, dei software e degli algoritmi, ovvero dalla crescente capacità di calcolo che può essere dedicata da soggetti malintenzionati nel tentativo di violare gli accessi.

La complessità minima delle chiavi SSH per l'accesso ai server segue la seguente pianificazione:

- Fino a novembre 2020 la complessità minima delle chiavi è RSA 2048.
- Da novembre 2020 in poi le chiavi RSA devono essere sostituite con chiavi a curva ellittica ECDSA o curve25519.
- Da marzo 2021 le chiavi per l'accesso ai server da parte degli amministratori di sistema devono risiedere su un token hardware protetto da PIN.

Per determinate operazioni (tra le quali la firma di pacchetti di installazione, la firma di tag sui sorgenti, la comunicazione di informazioni riservate tramite supporti non sicuri, ecc) Entaksi utilizza il sistema OpenPGP (RFC-4880) incluse le infrastrutture pubbliche di condivisione delle chiavi e dei livelli di fiducia reciproca tra i soggetti.

In alcuni contesti, ad esempio il backup dei sistemi, le informazioni devono essere cifrate utilizzando una password, anziché una chiava asimmetrica.

Le password utilizzate per questi scopi che non necessitano di essere conosciute da altri devono essere conservate dagli utenti in un file a sua volta cifrato, conservato nella propria postazione di lavoro e sottoposto a backup.

Per la gestione delle procedure crittografiche relative alla firma digitale valgono le norme e i regolamenti di legge definiti nella Unione Europea e nella legislazione nazionale italiana. In particolare:

- Il Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio - eIDAS.
- Il Codice dell'Amministrazione Digitale (Decreto Legislativo del 7 marzo 2005, n. 82, e successive modifiche).

Fino al 31/12/2021 sono state applicate le seguenti regole tecniche:

- Regole tecniche per la conservazione dei documenti informatici definite nel Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013.
- Regole tecniche sulla formazione dei documenti informatici definite nel .

Dal 01/01/2022 queste regole sono sostituite dalle seguenti:

- Regole tecniche per la sottoscrizione elettronica di documenti definite nelle Linee Guida dell'Agenzia per l'Italia Digitale ai sensi dell'art. 20 del CAD - 23 marzo 2020.

Gli algoritmi crittografici utilizzati nei processi che coinvolgono le firme digitali seguono le raccomandazioni contenute in ETSI TS 119 312.

7. Sicurezza fisica e ambientale

Entaksi Solutions SpA ha deciso di:

- **Posizionare in housing / hosting la maggior parte della sua infrastrutture server**.
  I server che ospitano ed erogano i vari servizi di cui la Società necessita per lo svolgimento delle sue attività, nonché quelli che vengono erogati ai propri clienti, sono collocati presso datacenter gestiti da fornitori specializzati allo scopo. La scelta dei datacenter viene revisionata periodicamente in funzione della dinamica del mercato, scegliendo di volta in volta le strutture che offrono il rapporto prestazioni/prezzo ritenuto più conveniente. Lo stesso criterio viene adottato per la fruizione di servizi generali di rete (quali ad esempio la risoluzione dei nomi a dominio e il relativo DNS), anch'essi affidati a servizi esterni.
- **Detenere la proprietà fisica di hardware coinvolti nell'erogazione di servizi fiduciari per i quali la normativa richiede il controllo diretto del Qualified Trust Service Provider**.
  Tali risorse hardware sono di proprietà dell'azienda e si trovano in un perimetro fisico al quale non hanno accesso altre organizzazioni, realizzato mediante un armadio dedicato sottoposto a un controllo degli accessi. Tali armadi sono messi a disposizione da fornitori specializzati, qualificati in ottemperanza alla normativa di settore.
- **Inquadrare in un rapporto di telelavoro tutti i dipendenti e collaboratori**.

Il risultato dell'adozione di questa impostazione è che la società opera totalmente in rete, senza dipendere da una sede operativa fisica centrale.

Perciò nell'organizzazione di Entaksi i controlli degli accessi sono gestiti secondo tre modalità:

- tramite il ricorso a verifiche di qualità che vengono eseguita in fase di qualifica dei fornitori e durante il monitoraggio dei servizi esterni utilizzati;
- tramite l'utilizzo di un ambiente sottoposto a controllo degli accessi;
- tramite l'applicazione dei controlli relativi alla sicurezza delle informazioni, in special modo agli asset affidati ai singoli dipendenti.

È necessario d'altra parte sottolineare che, dal punto di vista della sicurezza fisica delle infrastrutture centrali, quella che per Entaksi è stata una scelta di avanguardia in uno scenario dominato dalla gestione in proprio dei server, oggi è una tendenza ampiamente assodata che con sempre maggiore frequenza vede la migrazione in cloud come il modo più sicuro per gestire i servizi.

Entaksi garantisce il rispetto di requisiti minimi nella gestione della sicurezza fisica della infrastruttura centrale mediante i processi di qualifica e quello di monitoraggio dei fornitori che sono selezionati sia sulla base della convenienza di mercato che sulle garanzie di qualità offerte in tema di sicurezza, quali ad esempio la certificazione ISO/IEC 27001:2013 e, se necessario, la disponibilità ad essere sottoposti ad audit e ispezioni per riscontrare eventuali elementi non sufficientemente coperti dalle condizioni contrattuali o dalle certificazioni stesse.

Analoga considerazione, mutando il contesto, vale per le postazioni di lavoro, nella maggior parte dispositivi portatili affidati a dipendenti e collaboratori. In questo caso l'adozione di comportamenti corretti nella gestione del dispositivo e l'adozione di una serie di contromisure relative alla protezione logica dello stesso, quali ad esempio la gestione dell'accesso logico e la cifratura forte dei supporti di memorizzazione, consentono di garantire una adeguata protezione fisica delle infrastrutture periferiche e, laddove queste dovessero comunque essere violate, la possibilità di assumere il rischio di perdere il dispositivo senza che questo evento possa aprire vulnerabilità nel sistema, dato che esso risulterà inutilizzabile a terzi.

Tenendo conto di quanto esposto nei punti precedenti, Entaksi Solutions SpA ha deciso di impostare la sicurezza del proprio sistema informativo (e di conseguenza anche la continuità operativa, afferendo quest'ultima alla salvaguardia della disponibilità delle informazioni) assumendo convenzionalmente, nell'analisi dei rischi, il valore più alto per la probabilità che si possa verificare una minaccia di tipo 'fisico', e concentrando gli sforzi sulla minimizzazione dell'impatto che tali minacce possono determinare, ove si verifichino.

In altre parole, a seguito del verificarsi di una minaccia di tipo 'fisico', Entaksi considera accettabile il rischio del danno economico determinato sulle apparecchiature, purché questo non impatti sulla sicurezza del Sistema, sia per quanto riguarda la sicurezza delle informazioni ospitate o gestite dalle stesse, sia per quanto riguarda la continuità dei processi e la sicurezza della progettazione.

7.1. Aree protette

Vengono definite come "aree protette" tutte quelle aree che possiedono almeno una di queste caratteristiche:

- Aree in cui sono presenti le postazioni operative del sistema informativo, utilizzate dagli operatori per l'inserimento e la modifica di dati ("**Postazioni utente**").
- Aree in cui sono presenti postazioni dedicate allo sviluppo e test di applicativi software ("**Postazioni di sviluppo**").
- Aree in cui sono presenti apparecchiature critiche (server applicativi, basi dati, router etc.) del Sistema Informativo ("**Sale Server**").
- Aree in cui sono presenti apparecchiature che devono risiedere all'interno di un perimetro fisico ben definito, isolato e protetto, al quale l'accesso è precluso ad altre organizzazioni ed è soggetto a controllo e registrazione dei passaggi ("**Aree isolate**").

Le misure che si adottano per controllare l'accesso a tali "aree protette" sono tese a garantire un adeguato livello di sicurezza, che consenta l'ingresso e la permanenza nei locali esclusivamente del personale in turno di servizio o di personale autorizzato, prevenendo furti e danneggiamenti alle apparecchiature.

La postazione di lavoro per Entaksi è intesa come desktop, ma anche come scrivania, nel caso siano presenti documenti cartacei, e più in generale qualsiasi luogo nel quale siano contenute informazioni sensibili relative a processi aziendali, siano esse di proprietà di Entaksi, relative ai dipendenti, ai clienti o ai fornitori.

Le indicazioni generali per il mantenimento della postazione di lavoro sono le seguenti:

- la zona di lavoro deve essere costantemente presidiata, e resa sicura al termine della giornata di lavoro;
- le postazioni computer devono essere bloccate o spente quando non utilizzate;
- i dati cartacei devono essere resi inaccessibili a terzi quanto non si è presenti alla postazione;
- nel caso i dati, in qualsiasi forma, vengano conservati in luoghi chiusi a chiave, le chiavi non devono mai essere lasciate incustodite;
- le password non vanno mai scritte su foglietti lasciati accanto alla postazione di lavoro, e non vanno conservate in una posizione accessibile (anche un file sul computer non criptato è considerato accessibile).

In generale tutte queste indicazioni sono riconducibili alla politica di "schermo e scrivania puliti" ossia trattare gli spazi di lavoro in modo tale per cui non siano mai visibili informazioni sensibili, anche in maniera accidentale.
Al fine di proteggere tutti i dati sensibili e confidenziali Entaksi eroga ai suoi dipendenti formazione specifica su quali accorgimenti utilizzare affinché gli spazi di lavoro non rendano visibili informazioni sensibili.

7.2. Apparecchiature

Per quanto riguarda specificamente le apparecchiature le indicazioni sono le seguenti:

- i computer vanno impostati in modo che automaticamente si blocchino e richiedano la password dopo più di cinque minuti di inutilizzo;
- nel caso il proprio cellulare o altri dispositivi siano connessi ad attività aziendali (es. email) le regole per la postazione vengono estese anche ad essi;
- nel caso il cellulare sia connesso ad attività aziendale si richiede che esso sia protetto con un codice PIN di almeno 5 cifre, o lettura dell'impronta digitale, o disegno ad almeno 9 punti, ed è sconsigliato l'utilizzo del riconoscimento facciale;
- le sessioni sui sistemi gestiti da Entaksi hanno una durata massima di 30 minuti, dopo la quale la sessione risulta scaduta, in modo tale che in caso di sessioni lasciate aperte su altre dispositivi, venga impedito l'accesso a terzi: pertanto, al fine di rendere questa impostazione effettivamente operativa, è vietato memorizzare la password per servizi Entaksi su asset esterni a quelli in dotazione.

7.2.1. Documenti cartacei

Entaksi ha individuato un luogo sicuro ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, l'asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.

Il trattamento delle informazioni cartacee segue gli stessi principi delle informazioni elettroniche, e la loro protezione è da assicurarsi tramite il presidio dell'informazione (custodia in luogo sicuro) e in modo che il suo trasporto non ne metta a repentaglio la riservatezza, l'integrità e la disponibilità. Pertanto:

- i documenti cartacei vanno custoditi in un luogo sicuro;
- per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi;
- tutte le informazioni stampate devono essere rimosse dalla stampante non appena prodotte;

- i dispositivi quali stampanti e fotocopiatrici vanno controllati, in modo che non trattengano informazioni (es.: alcune stampanti hanno una cache che potrebbe memorizzare i file stampati);
- una volta terminata la loro funzione i documenti cartacei contenenti informazioni sensibili devono essere triturati, in maniera tale da rendere il loro contenuto illeggibile.

8. Sicurezza delle attività operative

Entaksi adotta una serie di misure per prevenire i rischi di interruzione delle proprie attività operative, rischi che possono derivare dall'esposizione degli asset e delle informazioni contenute proprio in ragione del loro utilizzo durante lo svolgimento di queste attività.

A questo scopo Entaksi definisce una serie di politiche di sicurezza che riguardano vari aspetti della gestione dei dispositivi e dei sistemi in particolare:

- le disposizioni sulle modalità di accesso ai sistemi;
- le disposizioni sull'uso dei dispositivi;
- le disposizioni sulla gestione e conservazione dei log di accesso.

8.1. Procedure operative e responsabilità

Entaksi assicura la correttezza nella gestione delle informazioni attraverso un insieme di procedure operative e alla formazione continua del personale sulla loro applicazione.

Le procedure definiscono in modo dettagliato ruoli e responsabilità nello svolgimento delle operazioni e prevedono una gestione della politica dei cambiamenti in modo da evidenziare ogni modifica che potrebbe avere impatto sulla sicurezza delle informazioni.

8.2. Sviluppo sicuro

Entaksi ritiene che la sicurezza nello sviluppo delle applicazioni debba essere considerata componente essenziale delle procedure di progettazione e realizzazione dei prodotti e servizi, dalla iniziale analisi dei rischi, alla espressione dei requisiti, alla esecuzione dei test intermedi, fino ai test definitivi di rilascio.

Le procedure operative che implementano e regolano le vari fasi della progettazione, sviluppo e rilascio di prodotti, servizi e delle stesse procedure del Sistema Integrato di Gestione devono quindi recepire questa impostazione, trasformandola, in relazione alle varie fasi, in prassi adeguate alla dimensione ed alle necessità operative della struttura.

La politica di sviluppo sicuro prevede inoltre il rispetto dei regolamenti che definiscono la visibilità dei dati, la registrazione delle autorizzazioni per il loro trattamento, la pseudonimizzazione dei dati personali. In fase di sviluppo, progettazione e verifica di qualità viene ridotto al minimo indispensabile l'utilizzo di dati personali, mediante tutte le misure tecniche e organizzative disponibili.

Qualora per esigenze di test sia necessario utilizzare dati personali non anonimizzati l'ambiente di test viene sottoposto agli stessi criteri di protezione dell'ambiente di produzione. Le informazioni personali sono sempre segregate in base al cliente interessato al trattamento dei dati, e non sono condivise se non previa autorizzazione degli interessati.

8.3. Separazione degli ambienti

L'attività di sviluppo di prodotti e servizi operata da Entaksi utilizza la separazione degli ambienti allo scopo di ridurre il rischio di distribuire in produzione prodotti e servizi che contengono modifiche non autorizzate.

Si distinguono in particolare:

- l'ambiente di produzione;
- l'ambiente di test, speculare a quello di produzione dove possono essere eseguite delle prove sui servizi con dati fittizi;
- l'ambiente di stage o validazione, dove vengono eseguire le verifiche di corrispondenza ai requisiti delle modifiche apportate a prodotti e servizi;
- l'ambiente di sviluppo, dove vengono provate le versioni preliminari di prodotti e servizi.

8.4. Privacy by design e privacy by default

In base all'art. 25 del Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati, Entaksi applica la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita, come riportato anche dal comma primo dell'articolo:

"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone

fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati."

Entaksi, in qualità di titolare o responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Al fine di poter meglio garantire tali obiettivi Entaksi ha ottenuto l'estensione della propria certificazione ISO/IEC 27001:2013 per la sicurezza delle informazioni alle ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

8.5. Protezione da virus, malware, ransomware

Gli attacchi informatici basati sulla diffusione di virus, malware e ransomware rappresentano un concreto di rischio per la sicurezza delle informazioni a tutti i livelli dell'infrastruttura, dai server, alle postazioni, ai dispositivi mobili.

La strategia di Entaksi per la riduzione di questo rischio si basa su una serie di contromisure di natura preventiva, difensiva e di intervento per il contenimento del danno.

Le misure preventive adottate sono:

- Privilegiare l'uso di sistemi operativi progettati per la sicurezza. I sistemi operativi considerati idonei sono GNU/Linux, Apple macOS, Microsoft Windows dalla versione 10 in poi
- Mantenere aggiornati i sistemi operativi con l'ultimo livello di patch disponibile presso fonti affidabili del produttore
- Privilegiare l'uso di software *open source* di cui è possibile verificare la sicurezza e l'affidabilità di concerto con la comunità di sviluppatori e utenti

Le misure difensive adottate sono:

- Utilizzare e mantenere aggiornate le soluzioni antivirus disponibili.
- Il controllo periodico sul software e sull'archivio dei documenti.

Le misure di intervento per il contenimento del danno sono:

- L'isolamento immediato dei dispositivi su cui viene rilevato un virus, malware o ransomware.
- La disattivazione delle credenziali degli utenti potenzialmente violate a causa della compromissione del dispositivo.
- Il ripristino completo del dispositivo compromesso evitando operazioni di recupero.

8.6. Backup

Entaksi adotta una politica di backup allo scopo di conservare copie di riserva dei dati, dei sistemi e delle loro configurazioni.

8.7. Raccolta dei log e monitoraggio

Entaksi dispone di una procedura di gestione del monitoraggio, dei log di sistema e dei log applicativi. Queste informazioni vengono sistematicamente raccolte, rese immodificabili e archiviate utilizzando una specifica impostazione delle regole di scarto.

8.8. Log di amministratori e operatori

I sistemi che prevedono l'accesso a basso livello per operazioni amministrative riservate agli amministratori di sistema dispongono di un log che traccia questi accessi.

8.9. Controllo del software di produzione

Entaksi adotta una politica di versionamento che consente di identificare univocamente il software installato sui sistemi in produzione e conserva gli eseguibili di ciascuna versione in appositi repository che garantiscono la corrispondenza della versione con il sorgente utilizzato per generarla.

8.10. Gestione delle vulnerabilità tecniche

Entaksi adotta una politica di sviluppo orientata alla sicurezza e alla privacy come requisiti principali. In questo contesto rientrano tutte quelle misure che consentono di mitigare l'impatto delle vulnerabilità tecniche, quali:

- La verifica su database pubblici delle vulnerabilità note sulle librerie utilizzate nello sviluppo;
- l'adozione sistematica di protocolli sicuri per le comunicazioni;
- l'utilizzo di una procedura di gestione degli incidenti di sicurezza;
- la gestione di un database di software autorizzati per le postazioni degli utenti;
- la conduzione, da parte di società terze specializzate, di verifiche delle vulnerabilità e test di penetrazione sui sistemi.

8.11. Considerazioni sull'audit dei sistemi informativi

Entaksi conduce annualmente un audit interno e uno operato da enti di certificazione accreditati per verificare la corrispondenza dei propri sistemi alle normative di sicurezza.

Entaksi è inoltre regolarmente sottoposta ad audit da parte di clienti che adottano questa politica nella loro procedura di accreditamento dei fornitori.

9. Sicurezza delle comunicazioni

Nella funzionalità del sistema i vari componenti comunicano tra di loro e con i client operati dagli utenti tramite protocolli applicativi che trasmettono messaggi tra un sistema e l'altro.

Per proteggere le transazioni effettuate tramite questi servizi applicativi e in particolare prevenire possibili indirizzamenti errati, alterazioni, trasmissioni incomplete o divulgazione non autorizzata dei messaggi, vengono scelti dei protocolli applicativi in grado di garantire questa protezione.

In particolare:

- Tutte le connessioni ai servizi applicativi avvengono esclusivamente con protocollo cifrato TLS, tramite connessione SSH o tramite una VPN cifrata.
- I protocolli applicativi utilizzati devono prevedere la gestione dell'integrità dei messaggi o, in alternativa, questa integrità deve essere garantita a livello applicativo.

La sicurezza delle comunicazioni è totalmente garantita a livello di trasporto in modo da rendere ininfluente ogni misura relativa alla protezione delle comunicazioni a livello di connessione fisica, ovvero sulle reti locali LAN, ethernet o Wi-Fi.

A livello di protocollo le connessioni sono protette mediante il sistema di Single Sign-On Entaksi utilizzando OpenID Connect per autenticare l'apertura della sessione ad esclusione di un numero limitato di applicazioni per le quali, per restrizioni tecniche, è necessario ricorrere all'autenticazione basata su utente e password.

Le comunicazioni tra servizi utilizzano, in ordine di priorità:

1. L'autenticazione OAuth2 impersonando l'identità del servizio appositamente definita.
2. L'autenticazione basata su API Token o utente e password di adeguata complessità.
3. La mutua autenticazione TLS.

10. Acquisizione, sviluppo e manutenzione dei sistemi

10.1. Requisiti di sicurezza dei sistemi informativi

Entaksi definisce regolarmente tra i requisiti non funzionali dei suoi prodotti e servizi il livello e la politica di sicurezza che devono essere rispettati durante lo sviluppo.

Questo approccio si applica sia allo sviluppo di nuovi servizi che all'aggiornamento di quelli esistenti in modo da tenere costantemente aggiornati i sistemi rispetto alla possibile obsolescenza di implementazioni di sicurezza datate.

10.2. Sicurezza nei processi di sviluppo e supporto

Nei processi di sviluppo e supporto i requisiti di sicurezza vengono implementati nei diversi moduli del sistema. In seguito le modifiche a questi moduli sono sottoposte ad una formale politica di gestione dei cambiamenti che include il tracciamento puntuale delle modifiche eseguite e, quando necessario, un'analisi dei rischi orientata a valutare se le modifiche possono includere violazioni di questi requisiti o introdurre delle vulnerabilità.

La progettazione dei sistemi e dei software tiene conto dello stato dell'arte per l'adozione delle migliori pratiche per lo sviluppo sicuro, ad esempio le linee guida pubblicata dal consorzio OWASP.

10.3. Dati di test

I dati di test utilizzati durante lo sviluppo, la validazione e il test dei sistemi e degli applicativi sono di norma protetti al pari dei dati di produzione, tuttavia questi dati sono sempre composti da informazioni fittizie o rese anonime mediante la mascheratura o l'alterazione delle parti sensibili.

I dati di test, pur mascherati e privati delle parti sensibili, sono comunque ridotti al minimo indispensabile per la conduzione delle attività di sviluppo, test e validazione.

11. Relazioni con i fornitori

Entaksi dispone di una procedura specifica per definire le modalità di gestione delle relazioni con fornitori. Questa procedura comprende una fasi di qualifica del fornitore che, a seconda del tipo di fornitura, può comprendere la verifica dei requisiti di sicurezza, fino alla possibilità di eseguire un audit per riscontrare il rispetto di questi requisiti.

11.1. Sicurezza delle informazioni nelle relazioni con i fornitori

Quando necessario Entaksi stabilisce accordi di riservatezza dettagliati sullo scambio di informazioni con i fornitori e verifica le condizioni in cui si applicano le prescrizioni dettate dall'art. 28 del Regolamento UE 2016/679 relativamente al trattamento dei dati.

11.2. Gestione dell'erogazione dei servizi dei fornitori

Entaksi sottopone a monitoraggio le prestazioni dei servizi erogati dai fornitori al fine di verificare se questi rientrano negli accordi sul livello di servizio stabiliti.

I fornitori sono inclusi nell'analisi dei rischi che Entaksi conduce regolarmente sull'insieme dei propri sistemi al fine di verificare le criticità e le possibilità di interscambio tra fornitori concorrenti.

12. Gestione degli incidenti relativi alla sicurezza delle informazioni

Si definisce "incidente di sicurezza" qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate o in transito, o che violi le politiche di sicurezza definite o le leggi in vigore, con particolare riferimento al Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati.

Il Team di risposta agli incidenti (Incident Response Team, IRT) è un gruppo di membri dell'organizzazione adeguatamente qualificati e di fiducia che gestisce gli incidenti durante il loro ciclo di vita.

Le procedure di gestione degli incidenti sono conformi alla norma ISO/IEC 27035:2016. Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- **Pianificare e preparare** - si stabilisce una politica di gestione degli incidenti di sicurezza delle informazioni, viene formato un IRT, l'organizzazione si prepara a rispondere a qualsiasi evento dannoso.
- **Rilevazione e segnalazione**: vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità.
- **Valutazione e decisione**: l'IRT verifica l'attendibilità e nel caso l'incidente venga confermato lo qualifica.
- **Risposta**: vengono attuate le contromisure, allo scopo di minimizzare i danni causati dall'incidente, se necessario vengono adeguate le risorse, e si procede al ripristino.
- **Attività successive**: viene aggiornata l'analisi dei rischi e verificata l'adeguatezza delle procedure di gestione degli incidenti
- **Lezioni apprese**: la Direzione revisiona l'incidente e vengono identificati i possibili punti di miglioramento.

13. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

I seguenti paragrafi descrivono come viene garantita la sicurezza delle informazioni durante l'applicazione delle procedure di continuità operativa di Entaksi.

13.1. Continuità della sicurezza delle informazioni

La continuità della sicurezza delle informazioni è parte integrante dei requisiti utilizzati nelle procedure di continuità operativa dei sistemi Entaksi.

Tali requisiti tengono conto delle speciali condizioni in cui l'organizzazione deve operare in caso di emergenza causata da guasti, crisi o eventi disastrosi che rendono l'infrastruttura informatica indisponibile, parzialmente disponibile o a rischio di distruzione.

Il personale viene formato e le procedure sottoposte a test allo scopo di fronteggiare le eventuali condizioni avverse nell'ambito di una operatività la cui efficacia è già stata verificata.

A questo scopo Entaksi dispone di un IRT composto dal personale con le competenze e le autorizzazioni per affrontare le situazioni di incidente di concerto con la DIR con una divisione predefinita di responsabilità e compiti.

Entaksi utilizza a tutti i livelli architetture ad alta affidabilità che replicano le funzionalità critiche in più istanze in modo che l'indisponibilità di un singolo sistema non comporti l'interruzione dei servizi.

13.2. Ridondanze

Entaksi utilizza sistemi ridondanti per assicurare la continuità operativa e pone particolare attenzione alla ridondanza dei dati, che sono distribuiti su più siti geograficamente distanti con ruolo paritetico, ovvero che possono operare indifferentemente come sito primario o come sito di disaster recovery in modo intercambiabile. I siti che ospitano le informazioni del sistema di conservazione sono riportati nei manuali del servizio.

Un sistema di backup completa in ogni caso le misure di sicurezza delle informazioni conservando le copie di ripristino del sistema. L'ubicazione del sito che ospita il backup è riportata nei documenti di sicurezza interni.

14. Conformità

14.1. Conformità ai requisiti cogenti e contrattuali

La Società, nella persona dei vari dirigenti responsabili, esegue un monitoraggio continuo sugli aggiornamenti legali e normativi di interesse per le attività aziendali, per i prodotti ed i servizi erogati, che possono dunque avere ripercussioni sull'intero Sistema Integrato di Gestione o su alcune sue parti.
Il monitoraggio è effettuato tramite la regolare frequentazione di gruppi di interesse stabiliti su vari canali social, attraverso il contatto personale dei vari responsabili con omologhi di altre aziende e con la partecipazione ad eventi istituzionali o promossi da organizzazioni private.

14.2. Miglioramento continuo

Tenendo come riferimento il Ciclo di Deming e il "risk-based thinking", la Direzione, sulla base dei risultati delle attività, delle risultanze degli Audit Interni, dell'analisi delle indicazioni provenienti dalle Parti Interessate, di eventuali reclami e ricorsi, monitora e governa con continuità le attività di miglioramento del Sistema Integrato di Gestione e dei processi da questo presidiati.

14.3. Riesame e audit

La Direzione analizza periodicamente l'idoneità, l'adeguatezza e l'efficacia del SIG. I risultati del riesame evidenziano bisogni e opportunità di miglioramento.

Le procedure di riesame e di audit si occupano in particolare di controllare se il SIG sia attuato in modo efficace e adeguato ai rischi a cui è sottoposta l'organizzazione.

Il SIG viene riesaminato nella sua interezza almeno annualmente, e il Responsabile del SIG può condurre ulteriori riesami qualora lo ritenga necessario, in ragione di intervenute modifiche straordinarie.

Oltre alle attività di verifica interne sono programmati e condotti anche gli audit esterni, al fine di ottenere le certificazioni e altri attestati di conformità periodici per il SIG e il Sistema di Conservazione.

Le verifiche vengono pianificate su base annuale dal Responsabile del SIG, che si preoccupa anche nei mesi precedenti all'incontro di verificare l'adeguatezza del SIG al programma di audit, e procede nel caso sia necessario agli eventuali aggiornamenti richiesti per il Sistema.

Per la conduzione degli audit esterni sono scelti, seguendo i principi elencati nella procedura interna di qualifica fornitori "PRO SIG 20200501 Fornitori", gli enti di certificazione accreditati da ACCREDIA, e, per quanto riguarda il Sistema di Conservazione, quelli indicati come idonei dall'Agenzia per l'Italia Digitale.

La revisione e l'eventuale aggiornamento di questa Politica per la Sicurezza delle Informazioni è effettuato dalla DIR in concomitanza con gli audit esterni di ricertificazione dei sottosistemi che lo compongono.