tinexta visura

PL 01.01
Politica per la sicurezza delle informazioni

tinexta visura

Riservatezza del documento

Il presente documento è classificato come:

TLP:GREEN

Legenda dei livelli di riservatezza del documento

Etichetta TLP	Come può essere condiviso?
TLP:RED	Di non divulgazione, informazione ristretta ai soli partecipanti.
TLP:AMBER	Divulgazione limitata alle sole organizzazioni coinvolte e i propri clienti.
TLP:AMBER+STRICT	Divulgazione limitata alle sole organizzazioni coinvolte.
TLP:GREEN	Divulgazione limitata ai soli appartenenti alla comunità.
TLP:CLEAR	Divulgazione illimitata.

Le modalità di classificazione e il significato delle etichette TLP sono spiegati in maggiore dettaglio nella procedura "PR 03 - Classificazione ed etichettatura delle informazioni"

tinexta visura

Ultime Versioni del documento

VERSIONE N.	DATA DI APPROVAZIONE	AUTORE
00	06/07/2024	Consulente esterno (Corvallis)
		VERIFICATA DA
	07/01/2025	Edoardo Ballacci (S.Q.A. Consulting) Fabrizio Virgilio
	04/02/2025	Funzione Compliance
		APPROVATA DA
	24/07/2025	Andrea Vingolo
DESCRIZIONE MODIFICA	Prima emissione	

VERSIONE N.	DATA DI APPROVAZIONE	AUTORE
01	07/11/2025	Fabrizio Virgilio
		VERIFICATA DA
	13/11/2025	Funzione Compliance
		APPROVATA DA
	14/11/2025	Andrea Vingolo
DESCRIZIONE MODIFICA	Adeguamento classificazione riservatezza a standard TLP	

Riferimenti Normativi

Documenti di riferimento	
UNI EN ISO 27001:2022	Punto 5.2

tinexta visura

Documenti correlati

Il presente documento è armonizzato con i seguenti documenti di origine interna:

- DOC 01 - Manuale del SGSI
- DOC 02 - Contesto dell'Organizzazione
- DOC 03 - Obiettivi per la sicurezza delle informazioni
- DOC 04 - Riesame della direzione
- DOC 07 - Verbale di Audit
- PL 01 - Politica per la sicurezza delle informazioni
- PR 12 - Protezione e cancellazione dei record
- REG 01 - Elenco documenti a sistema
- REG 02 - Dichiarazione di Applicabilità (SOA
- REG 03 - Analisi del rischio
- REG 04 - Indicatori chiave di processo (KPI
- REG 09 - Piano annuale di Audit

Sommario

1 Premessa

Tinexta Visura S.p.A. (di seguito anche "Società", "Azienda", "Organizzazione" o "Visura") è specializzata nello sviluppo e gestione di piattaforme applicative finalizzate all'erogazione di servizi relativi al Processo Telematico per le professioni forensi, all'erogazione di servizi per la digitalizzazione dei processi interni ad Enti e Ordini Professionali, Pubblica Amministrazione e persone fisiche e giuridiche.
La Società ha fondato la propria politica e il proprio modo di operare sui principi cardine dell'efficienza e dell'efficacia, garantendo la trasparenza dei processi operativi, lavorando sulla responsabilizzazione

dei propri operatori, nell'ottica della semplificazione delle procedure, della facilità di accesso da parte dei fruitori dei servizi e nel rispetto della sicurezza delle informazioni gestite.

Obiettivo primario dell'Organizzazione nell'ambito della sicurezza delle informazioni è garantire:

1) la raccolta, l'interpretazione delle esigenze operative e la definizione di opportune policy per la gestione delle soluzioni applicative;
2) il governo delle infrastrutture tecnologiche intese come fattore abilitante delle soluzioni messe a punto dall'area applicativa.

L'obiettivo principale si concretizza nel perseguimento del fine aziendale: fornire con rapidità e prontezza tutte le risposte che l'utenza richiede attraverso un costante contatto con il cliente, tramite il conseguimento dei seguenti obiettivi:

- qualità e disponibilità del servizio concordato;
- efficacia dei metodi preventivi e reattivi per la verifica dello stato di sicurezza;
- efficacia dei metodi relativi alla gestione e configurazione dei dispositivi di sicurezza;
- efficacia dei metodi preventivi e reattivi per la gestione degli incidenti di sicurezza;
- ascolto attivo dell'utenza per un servizio di qualità;
- trasparenza dei Processi IT;
- miglioramento continuo ed innovazione;
- garanzia della continuità del business attraverso la protezione ed il tempestivo recupero dei processi critici dagli effetti di malfunzionamenti dei Sistemi Informativi o di disastri.

Data l'importanza strategica della sicurezza delle informazioni, delle reti e dei sistemi IT, Visura si è dotata di una politica di alto livello per strutturare le linee guida di un percorso volto al miglioramento della gestione della sicurezza delle informazioni.

2 Enunciato

La gestione della sicurezza delle informazioni costituisce una priorità di alto livello all'interno della "Mission" aziendale, ove si attribuisce importanza strategica al trattamento delle informazioni e concretizza la volontà di difendere la riservatezza, l'integrità e la disponibilità dei dati.

Per questo scopo, l'Organizzazione riconosce la necessità di sviluppare, mantenere, controllare e migliorare in modo costante un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in conformità alla norma ISO 27001:2022.

Gli obiettivi principali del SGSI si concretizzano nell'assicurare:

- la riservatezza del patrimonio informativo gestito: l'informazione non è resa disponibile o comunicata ad individui, entità o per processi non autorizzati;
- l'integrità del patrimonio informativo gestito: tutelare l'accuratezza e la completezza degli asset, ossia di qualsiasi informazione o bene attinente a cui Visura attribuisce un valore;

- la disponibilità del patrimonio informativo gestito: l'informazione deve essere accessibile ed utilizzabile previa richiesta di una entità autorizzata;
- l'ottemperanza ai requisiti cogenti, del quadro normativo di riferimento e contrattuali;
- l'ottemperanza ai requisiti di business ed a quanto imposto dal rischio definito nel contesto in cui l'Azienda si trova ad operare;
- la redazione di piani per la continuità della sicurezza della informazione della Società, e che tali piani siano il più possibile tenuti aggiornati e controllati;
- l'adeguata formazione del personale in tema di sicurezza delle informazioni;
- la corretta gestione di tutte le violazioni della sicurezza delle informazioni e dei possibili punti deboli, al fine di una corretta rilevazione ed indagine.

In questa ottica, Visura è consapevole che la sicurezza delle informazioni è un processo culturale complesso che deve coinvolgere tutte le risorse umane ed organizzative. L'Azienda è, altresì, consapevole del ruolo della tecnologia a supporto dei processi di sicurezza delle informazioni e, pertanto, promuove le soluzioni tecniche e/o tecnologiche applicabili al proprio contesto/modello operativo di riferimento.

Il fine ultimo, come detto, è perseguire gli obiettivi principali di un SGSI ovvero la ***riservatezza****, la* ***disponibilità*** *e* ***l'integrità*** *delle informazioni.*

2.1 Applicabilità

La Politica per la Sicurezza delle Informazioni si applica:

- a tutto il personale aziendale (compresi collaboratori);
- ai Partners, ai Fornitori o Terze Parti coinvolti nel trattamento delle informazioni o a cui i documenti del SGSI vengono diffusi;
- a coloro che abbiano accesso agli uffici e/o all'infrastruttura di Visura.

2.2 Obiettivi

Visura si propone il raggiungimento dei seguenti obiettivi:

- applicare periodicamente una metodologia di valutazione del rischio adeguata al SGSI, ai requisiti di business individuati, a quelli cogenti e normativi;
- identificare, attraverso una idonea analisi dei rischi, il valore del patrimonio informativo all'interno del campo di applicazione del SGSI al fine di comprendere le vulnerabilità e le possibili minacce che possano esporlo a rischi;
- gestire il rischio ad un livello accettabile ed in modo allineato al più generale contesto di gestione del rischio strategico dell'Organizzazione;
- definire e rendere effettive le linee operative per una architettura di sicurezza, intesa come: l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscano - in ogni struttura organizzativa, ambiente informatico, singolo elaboratore - il rispetto degli standard definiti dall'Azienda;

- controllare, cogliendo ogni spunto di miglioramento, il sistema attuato.

La sicurezza delle informazioni garantisce adeguatamente la riservatezza, la disponibilità e l'integrità (RID) e la verificabilità di tutti i tipi di informazioni (elettroniche, cartacee, orali) in conformità con i requisiti dei titolari delle informazioni.
Quando le informazioni viaggiano su supporti tecnologici, il loro controllo può sfuggire: è molto più immediato gestire fisicamente l'accesso ad un'area, ad un ufficio o ad un armadio piuttosto che verificare gli accessi alle cartelle di rete e alle aree virtuali condivise.
A ciò si aggiunge che l'emergenza Covid-19 ha reso necessario e improvviso il remote-working nella maggior parte delle aziende. Il contesto domestico è, per sua natura, molto meno sicuro degli uffici aziendali: router deboli, assenza di VPN o di firewall, PC non gestiti e utenti multipli rendono più vulnerabili i dati e le reti aziendali.

Archiviare e utilizzare informazioni elettroniche	
Vantaggi	Svantaggi
è possibile, comodamente dalla propria postazione, reperire le informazioni (anche quelle più *datate*)	occorre garantire l'accesso limitato ai documenti elettronici
è possibile accedere ad un numero cospicuo di documenti	occorre proteggere il contenuto delle informazioni da accesso abusivo, alterazione, furto
si riduce al minimo lo spazio di archiviazione *fisica* dei documenti	è necessario fare in modo che i documenti elettronici siano validi ed efficaci
minor costo per l'archiviazione e l'eliminazione dei dati	occorre fare in modo che i terzi possano avere accesso alle informazioni solo se sono autorizzate
miglioramento alla reputation: poter dimostrare di aver messo a punto tutte le misure necessarie per proteggere non solo i propri dati ma anche per contribuire a preservare i dati della filiera di cui si fa parte (clienti, fornitori, partner, ...)	occorre formare il personale interno relativamente alla digitalizzazione dei documenti, alla loro creazione, utilizzo e protezione
ottimizza l'allocazione del budget: grazie alla fotografia dello stato della *security posture*, la certificazione ISO 27001 permette di indirizzare gli investimenti in soluzioni di cyber security che riducono il rischio per il contesto specifico dell'azienda.	occorre stabilire ed applicare regole organizzative e tecniche per eliminare i file, trascorsi i termini di legge di archiviazione

La politica della sicurezza delle informazioni comprende 3 ambiti:

1. la protezione delle informazioni;
2. la sicurezza informatica;
3. la protezione dei dati.

Oltre ai dati personali di cui l'Azienda, per legge, è tenuta a garantire la sicurezza, esistono informazioni che rivestono un immenso valore economico. Tali informazioni, quindi, devono essere adeguatamente protette (a seconda del rischio). La necessità di protezione e i rischi determinano tutte le misure di sicurezza applicate.
La sicurezza delle informazioni è stabilita, gestita e migliorata costantemente nel SGSI. Essa costituisce un aspetto parziale della sicurezza integrale dell'Organizzazione andandosi ad integrare con la conformità alle leggi sulla privacy e al rispetto degli standard specifici dei propri clienti che l'Azienda deve rispettare.

La sicurezza informatica, in generale, consiste nell'assicurare che le risorse hardware e software siano usate unicamente nei casi e nei modi previsti dalle norme e dagli accordi intercorsi tra la parte e l'utente o tra una parte e l'altra.
L'obiettivo della sicurezza informatica è di garantire cinque aspetti dell'ICT:

1) l'integrità dei dati: devono effettivamente essere quelli che le parti in causa legittimamente sono convinti che siano;
2) la confidenzialità: solo le persone autorizzate devono poter accedere alle informazioni;
3) la disponibilità: coloro che ne hanno diritto devono poter sempre accedere alle informazioni;
4) il non ripudio: un'azione svolta non può essere negata a posteriori da un utente;
5) l'autenticazione: assicura l'identità digitale di un utente.

2.3 Responsabilità

La presente politica viene emessa e riesaminata dalla Direzione.
Il Responsabile SGSI definisce norme e procedure per l'attuazione della presente politica. Tutto il personale ed i fornitori devono seguire le procedure stabilite dal SGSI.
Fa parte, inoltre, della politica generale del SGSI identificare le responsabilità specifiche per la gestione della sicurezza delle informazioni rispetto ai ruoli definiti.

Tutto il personale, in base alle proprie conoscenze, ha la responsabilità di riferire al Responsabile SGSI qualsiasi punto debole individuato.

Visura garantisce che tutto il personale coinvolto nella sicurezza delle informazioni sia competente in quanto formalmente istruito e formato nonché che abbia competenze ed esperienza adeguate.
Le competenze richieste vengono determinate e riviste regolarmente insieme a una valutazione dei livelli di abilità esistenti. Sono individuate le esigenze in materia di formazione e viene mantenuto un piano per garantire l'esistenza delle competenze necessarie.
La formazione, l'istruzione e altri documenti pertinenti sono conservati dalla Funzione HR per documentare i livelli di abilità individuali raggiunti.

I contenuti dei documenti del SGSI riguardano tutti gli utenti.

La mancata applicazione delle prescrizioni da parte degli stakeholders interni potrà essere oggetto di procedimento sanzionatorio.

Per gli stakeholders esterni, la mancata applicazione del SGSI, a seconda della gravità e del pregiudizio subìto o subendo dalla Società, potrà comportare l'immediata risoluzione del rapporto e la richiesta di risarcimento del danno *ex lege*.

2.4 Riesame

La presente politica viene riesaminata regolarmente, almeno annualmente, e ogniqualvolta subentrino possibili modifiche che la influenzano, per accertarsi che rimanga idonea a perseguire il proprio scopo, alle aspettative degli utenti e di tutte le parti interessate.

Conformemente a quanto riportato nel Manuale del SGSI, ogni documento specifico è associato ad un responsabile che ha l'incarico di riesaminarlo e rivalutarlo periodicamente al fine di garantire che esso persegua le opportunità di miglioramento delle politiche di gestione delle informazioni e che gestisca il supporto ai cambiamenti del contesto organizzativo, di business, legali e tecnici.

2.5 Riferimenti agli aspetti cogenti e ai regolamenti

Per Visura riveste assoluta importanza l'idoneità ai requisiti cogenti e regolamentari.
La politica aziendale, in questo particolare ambito, si pone i seguenti obiettivi:

- assicurare che siano identificati ed aggiornati tutti i requisiti cogenti e regolamentari applicabili;
- assicurare che questi requisiti siano utilizzati come "dati di ingresso ai processi" e che ne sia riscontrata la conformità nell'ambito del monitoraggio sui "dati di uscita dai processi", con particolare riferimento alle attività di audit interno;
- assicurare che l'Organizzazione dimostri adeguatamente la conformità ai requisiti cogenti.

2.6 Criteri per l'accettazione del rischio e livelli di rischio

Al fine di allineare la presente politica con il contesto di gestione del rischio strategico dell'Organizzazione all'interno del quale avranno luogo l'impostazione e l'aggiornamento del SGSI e per stabilire i criteri con i quali ponderare il rischio viene, di seguito, descritta una tabella di valutazione del rischio.
I livelli di rischio definiti indicano i livelli in cui può essere compromesso il raggiungimento delle strategie e degli obiettivi aziendali.

Livello di Rischio	Valutazione
ALTO	Un rischio è inaccettabile qualora l'impatto abbia un effetto significativo sul raggiungimento degli obiettivi strategici, ad esempio: • Perdita di dati critici;

	• Dati e servizio non disponibile; • Perdita o significativa riduzione della credibilità/immagine nei confronti dei portatori di interesse; • Sanzioni penali a carico dei dipendenti. • Sanzioni da parte degli enti preposti alla tutela della privacy
MEDIO	Inefficienza delle normali operazioni con un effetto limitato sul raggiungimento degli obiettivi strategici, ad esempio: • interruzioni o significative inefficienze nel processo di gestione del servizio; • problemi temporanei di qualità/servizio; • inefficienze nei flussi e nelle operazioni.
BASSO	Nessun impatto concreto. Si tratta di situazioni diverse dalla norma che richiedono comunque valutazioni e azioni di miglioramento.

2.7 Comunicazione

La politica del SGSI è comunicata all'interno di Visura attraverso SharePoint e tramite apposite sessioni formative e comunicazioni da parte dell'Ente interno preposto.
La classificazione, e la conseguente etichettatura, fa sì che la Politica possa essere resa di pubblico dominio e, pertanto, condivisibile con gli stakeholders richiedenti. Nel caso, è fatto salvo il diritto della proprietà intellettuale in capo a Visura, come prescritto dalla norma (controllo A.5.32 ISO 27001:2022).

tinexta

visura

think next,
access now