PROTOCOLLO DI CYBERSECURITY

PER STUDI LEGALI

Gestione sicura di dati, comunicazioni e strumenti digitali

Applicabile a studi legali di qualsiasi dimensione

Centuria Foundation

centuriafoundation.pl

Versione 1.0 | 2025 | Licenza: CC BY-SA 4.0

Indice

1. Introduzione e Contesto

Gli studi legali trattano quotidianamente informazioni tra le piu sensibili: segreto professionale, dati personali e giudiziari dei clienti, strategie riservate, documenti di causa. Una violazione informatica non e solo un danno operativo: e una violazione del dovere deontologico.

Questo protocollo fornisce linee guida operative, metodologie e strumenti pratici per proteggere lo studio da minacce informatiche reali, con approccio scalabile per studi di qualsiasi dimensione.

1.1 Riferimenti Normativi

Norma / Regolamento	Rilevanza per lo Studio Legale
GDPR (Reg. UE 2016/679)	Protezione dati personali clienti. Obbligo di misure tecniche adeguate. Notifica data breach entro 72 ore.
D.Lgs. 196/2003	Codice Privacy italiano modificato dal GDPR. Regola il trattamento dati in ambito nazionale.
Codice Deontologico Forense	Artt. 28-29: obbligo di riservatezza e segreto professionale, applicabile anche agli strumenti digitali.
NIS2 (Dir. UE 2022/2555)	Dal 2024: studi con >50 dipendenti o con ruolo in infrastrutture critiche rientrano nell'ambito applicativo.
ISO/IEC 27001	Standard internazionale per la gestione della sicurezza delle informazioni. Riferimento per best practice.

Attenzione: Rischio Deontologico

Una violazione informatica che espone dati dei clienti puo configurare:

- Violazione del segreto professionale (art. 28 Codice Deontologico Forense)
- Responsabilita civile verso il cliente danneggiato
- Illecito amministrativo GDPR: fino a 20 milioni di euro o 4% del fatturato globale
- Segnalazione obbligatoria al Garante Privacy entro 72 ore dalla scoperta

La cybersecurity non e una questione meramente tecnica: e una questione professionale e deontologica.

2. Gestione di Password e Accessi

Le password deboli o riutilizzate sono la causa principale di compromissione degli account. Il principio guida: ogni account deve avere una password unica, lunga e generata casualmente.

2.1 Requisiti Minimi delle Password

Parametro	Requisito Minimo	Raccomandato
Lunghezza	16 caratteri	20+ caratteri
Composizione	Lettere, numeri, simboli	Stringa casuale completa
Riutilizzo	Vietato	Vietato in assoluto
Cambio periodico	Solo in caso di breach	Non cambiare senza motivo (NIST 2024)
Archiviazione	Solo tramite password manager	Mai su carta, email o file di testo

Nota metodologica: NIST SP 800-63B (2024)

Le linee guida NIST indicano che il cambio periodico forzato delle password e controproducente:

spinge gli utenti a creare password piu deboli e prevedibili.

La politica corretta: cambiare la password SOLO se si sospetta o conferma una compromissione.

2.2 Password Manager: Strumenti Raccomandati

Un password manager genera, archivia e compila automaticamente password uniche e casuali per ogni servizio. E lo strumento fondamentale per applicare la politica delle password.

Strumento	Tipo	Adatto a	Note
Bitwarden	Cloud / Open source	Studi di tutte le dimensioni	Gratuito; versione Business con controllo centralizzato
1Password	Cloud commerciale	Studi medi e grandi	Ottima gestione team; audit log incluso
KeePassXC	Locale / Open source	Singolo avvocato / piccolo studio	Nessun cloud; file locale da backuppare
Keeper	Cloud enterprise	Grandi studi	Compliance GDPR integrata; audit

			avanzato

2.3 Autenticazione a Due Fattori (2FA/MFA)

Il 2FA e obbligatorio per tutti i servizi critici. Anche se la password viene compromessa, il secondo fattore impedisce l'accesso non autorizzato.

Metodo 2FA	Sicurezza	Facilita d'uso	Raccomandazione
App Authenticator (TOTP)	Alta	Media	PRIMA SCELTA
Chiave hardware (FIDO2/YubiKey)	Massima	Alta	Raccomandato per accessi critici
SMS / telefonata	Bassa (SIM swap)	Alta	Evitare se possibile
Email come 2FA	Molto bassa	Alta	Non accettabile

App Authenticator raccomandate

- Aegis Authenticator (Android, open source, backup cifrato locale) - getaegis.app
- Raivo OTP (iOS, open source)
- 2FAS (iOS e Android, backup cloud opzionale)

Importante: generare e conservare SEMPRE i codici di ripristino 2FA in un luogo fisico sicuro. Perdere l'accesso al dispositivo 2FA senza codici di backup significa perdere l'account.

2.4 Segregazione degli Accessi: Principio del Minimo Privilegio

Ogni persona nello studio deve avere accesso solo alle risorse strettamente necessarie alla propria funzione. Mai dare accessi piu ampi del necessario.

Ruolo	Perimetro di accesso
Avvocato socio	Accesso completo ai propri fascicoli, gestione amministrativa dello studio
Collaboratore	Accesso ai fascicoli assegnati; nessun accesso a contabilita o dati altrui
Segreteria	Calendari, comunicazioni generali; non ai documenti di causa
Stagista / praticante	Accesso limitato ai fascicoli supervisionati; revocabile immediatamente

Procedura obbligatoria: Revoca degli Accessi

Al termine di ogni rapporto di collaborazione o impiego:

1. Revocare IMMEDIATAMENTE tutti gli accessi entro 24 ore dalla cessazione
2. Reimpostare le password condivise eventualmente conosciute
3. Verificare l'assenza di accessi residui (email, cloud, gestionale, VPN)
4. Documentare la revoca con data e firma del responsabile

Questa procedura e obbligatoria anche per stagisti e collaboratori occasionali.

3. Email e Comunicazioni con i Clienti

L'email e il vettore d'attacco numero uno negli studi professionali. Phishing, BEC (Business Email Compromise) e intercettazione di comunicazioni riservate sono minacce concrete e documentate nel settore legale.

3.1 Infrastruttura Email Sicura

Requisito	Descrizione
Dominio professionale dedicato	Mai usare indirizzi @gmail / @libero per comunicazioni professionali. Usare @nomestudio.it.
Record SPF	Configurare DNS SPF per impedire lo spoofing del dominio dello studio da parte di terzi.
DKIM	Firma digitale delle email in uscita. Garantisce l'autenticita del mittente.
DMARC	Politica di gestione delle email non autenticate. Protezione contro phishing verso i clienti.
TLS in transito	Cifratura del canale di trasmissione. Abilitato di default nei provider moderni (verificare).
Cifratura end-to-end	Per comunicazioni altamente riservate: S/MIME o PGP con il cliente (ove tecnicamente possibile).

3.2 Riconoscere il Phishing

Il phishing mirato verso studi legali (spear phishing) e sofisticato: i criminali studiano lo studio, i clienti e le cause in corso prima di colpire.

Segnali d'allarme: controllare sempre questi elementi

- Il nome visualizzato del mittente e diverso dall'indirizzo email reale
- Urgenza insolita: 'rispondere entro oggi', 'azione immediata richiesta'
- Richiesta di credenziali, bonifici o documenti via email
- Link che al passaggio del mouse mostrano URL diversi dal testo
- Allegati .zip, .exe, .iso, .lnk, o documenti Office con macro
- Email da un cliente noto con tono insolito o richieste inusuali
- Indirizzo reply-to diverso dal mittente originale

Regola d'oro: in caso di dubbio, chiamare il presunto mittente al numero GIA' in rubrica. Non usare il numero di telefono eventualmente indicato nella email sospetta.

3.3 BEC - Business Email Compromise

Il BEC e una truffa in cui l'attaccante compromette o impersona un account email legittimo per dirottare bonifici o ottenere documenti riservati.

- Verificare SEMPRE telefonicamente le coordinate bancarie ricevute via email prima di eseguire un bonifico
- Una email anche apparentemente autentica del cliente che cambia IBAN richiede verifica telefonica immediata
- Non fidarsi del tono familiare: l'account reale del cliente potrebbe essere compromesso
- Documentare per iscritto la procedura di verifica adottata

3.4 PEC - Posta Elettronica Certificata

La PEC ha valore legale in Italia per la certezza di consegna, ma non cifra il contenuto del messaggio. Non e equivalente a una comunicazione cifrata end-to-end.

- Usare la PEC per comunicazioni che richiedono certezza di consegna e data certa
- Non usare la PEC come unico strumento di sicurezza per contenuti altamente riservati
- Monitorare la casella PEC regolarmente: i termini processuali decorrono dalla ricezione
- Configurare 2FA sull'account PEC se il provider lo supporta

4. Archiviazione Documenti e Cloud

L'archiviazione sicura e una delle aree piu critiche per uno studio legale. I requisiti sono quattro: riservatezza, integrita, disponibilita e tracciabilita.

4.1 Criteri di Scelta per Soluzioni Cloud

Criterio	Requisito	Come verificare
Localizzazione dati	Server in UE (GDPR artt. 44-49)	Leggere T&C del provider
Cifratura at-rest	AES-256 o superiore	Documentazione tecnica
Cifratura in transito	TLS 1.2 minimo, 1.3 raccomandato	Test con SSL Labs
Log di accesso	Audit trail di chi accede e quando	Pannello di amministrazione
Backup e recovery	RPO/RTO documentati, test periodici	SLA del provider
DPA - Data Processing Agreement	Obbligatorio per fornitori che trattano dati GDPR	Contratto firmato con il provider

4.2 Soluzioni Raccomandate

Soluzione	Tipo	Adatta a	Note
Nextcloud (self-hosted)	Cloud privato open source	Tutti i livelli	Massimo controllo; richiede manutenzione
Microsoft 365 Business	Cloud enterprise	Studi medi / grandi	Server UE disponibili; DPA incluso
ProtonDrive	Cloud zero-knowledge	Singolo / piccolo studio	Server Svizzera; cifratura lato client
Tresorit	Cloud zero-knowledge EU	Tutti i livelli	Progettato per legal; E2E encryption

Cosa NON usare per documenti riservati dei clienti

- Google Drive / OneDrive account personale (dati fuori dal perimetro aziendale)
- Dropbox piano gratuito (server USA, nessun DPA standard)
- WeTransfer gratuito (nessuna garanzia di riservatezza)
- WhatsApp per trasferimento documenti (vedi sezione 6)
- USB / hard disk non cifrati per backup

Regola: se non si sa dove fisicamente risiedono i dati, non usare il servizio per dati riservati.

4.3 Classificazione dei Documenti

Livello	Contenuto tipico	Misure minime
RISERVATO	Atti giudiziari, pareri, segreto professionale, dati sensibili	Cifratura E2E, accesso nominale, log obbligatorio
CONFIDENZIALE	Corrispondenza clienti, contratti, documentazione di causa	Cloud cifrato, accesso limitato, nessuna condivisione non autorizzata
INTERNO	Procedure interne, comunicazioni tra colleghi	Rete interna o cloud aziendale; nessuna distribuzione esterna
PUBBLICO	Materiale promozionale, pubblicazioni	Nessuna restrizione particolare

4.4 Politica di Backup: Regola 3-2-1

- 3 copie dei dati (originale + 2 backup distinti)
- 2 supporti diversi (es. cloud + disco esterno cifrato)
- 1 copia off-site o geograficamente separata

- I backup vanno testati periodicamente con ripristino reale, non solo verifica file
- I backup devono essere cifrati, specialmente quelli su supporto fisico
- Frequenza raccomandata: giornaliera per dati attivi, settimanale per archivio

5. Dispositivi Mobili e Smart Working

Il lavoro da remoto e l'uso di dispositivi mobili hanno ampliato enormemente la superficie di attacco. Un dispositivo non protetto usato fuori dall'ufficio e un rischio concreto per l'intero studio.

5.1 Configurazione Minima dei Dispositivi

Misura	Smartphone	PC / Laptop
Cifratura del disco	Attiva di default (iOS/Android)	BitLocker (Windows) / FileVault (Mac)
PIN / password di blocco	Minimo 6 cifre; biometria OK	Password sicura; blocco automatico 5 min
Aggiornamenti OS	Automatici abilitati	Aggiornamenti critici entro 48h
Antivirus / EDR	N/A (iOS/Android sandboxed)	Obbligatorio: EDR o antivirus aggiornato
VPN	Su reti non fidate (Wi-Fi pubblici)	Obbligatoria fuori dall'ufficio
Cancellazione remota	Configurare Find My / Google Find	MDM o soluzione endpoint management

5.2 Segregazione del Dispositivo Mobile

La commistione tra uso professionale e personale dello smartphone crea rischi concreti e documentati.

Rischi della commistione professionale / personale

- App personali con accesso ai contatti professionali (es. WhatsApp carica l'intera rubrica)
- Backup automatici che includono documenti riservati in cloud personali
- App di gaming / social che raccolgono dati dal dispositivo
- Familiari che usano il dispositivo: accesso indiretto ai dati dei clienti
- Furto / smarrimento espone simultaneamente vita privata e dati professionali

Opzione A: Dispositivo Fisicamente Separato (raccomandata)

- Smartphone dedicato esclusivamente all'uso professionale
- Nessuna app personale (social, gaming, shopping, banking personale)
- Backup separato, gestito e cifrato dallo studio
- Costo indicativo: 200-500 euro/anno; ampiamente giustificato dal rischio gestito

Opzione B: Work Profile sullo stesso dispositivo

- Android: Work Profile (separa completamente app e dati professionali dai personali)
- iOS: gestione tramite MDM (Mobile Device Management) con container separato
- I dati del profilo professionale sono isolati e cancellabili separatamente
- Soluzione accettabile; preferibile a nessuna segregazione

5.3 Wi-Fi e Reti Esterne

- Non connettersi mai a Wi-Fi pubblici (aeroporti, hotel, bar, coworking) senza VPN attiva
- Preferire hotspot mobile personale (4G/5G) per lavoro urgente fuori ufficio
- Nella rete dello studio: separare Wi-Fi ospiti dalla rete di lavoro
- Cambiare la password del router ogni 12 mesi; disabilitare WPS

6. Comunicazioni con i Clienti e Uso dell'Intelligenza Artificiale

6.1 Canali di Comunicazione: Confronto

Canale	Cifratura	Valutazione	Condizioni d'uso
Signal/Molly	End-to-end (E2E)	PRIMA SCELTA	Comunicazioni riservate; cliente deve accettare di usarlo
Email + S/MIME / PGP	E2E se configurato	CONSIGLIATO	Per clienti con certificato o chiave pubblica configurata
Email standard (TLS)	Solo in transito	ACCETTABILE	Comunicazioni ordinarie; non per dati RISERVATI
WhatsApp	E2E (protocol Signal)	CON CAUTELA	Metadata condivisi con Meta; backup cloud non cifrato di default
Telegram	Solo in transito (default)	EVITARE	Chat normali NON sono E2E; solo 'secret chats' lo sono
SMS	Nessuna	NON USARE	Intercettabile; nessuna riservatezza

6.2 Intelligenza Artificiale Generativa: Linee Guida

L'uso di strumenti AI (ChatGPT, Claude, Gemini, Copilot, ecc.) negli studi legali e in rapida crescita. Crea pero rischi specifici che devono essere compresi e gestiti con regole esplicite.

Rischi principali dell'uso AI in ambito legale

Rischio	Descrizione
Data leakage	Dati inseriti nel prompt possono essere usati per training o visualizzati da operatori del provider.
Allucinazioni legali	L'AI puo inventare sentenze, articoli di legge e precedenti inesistenti con aspetto convincente.
Responsabilita professionale	L'avvocato firma e resta responsabile del contenuto prodotto, anche se generato da AI.
Violazione segreto professionale	Inserire dati identificativi del cliente in un'AI cloud puo configurare violazione del segreto.
Dipendenza e deskilling	Uso acritico dell'AI riduce nel tempo la capacita di valutazione autonoma.

Politica d'uso dell'AI: Regole operative dello studio
VIETATO inserire nei prompt AI:

- Nomi, cognomi, codici fiscali o qualsiasi identificativo del cliente
- Dettagli specifici di cause in corso o atti non pubblici
- Coordinate bancarie, dati sanitari, dati giudiziari
- Qualsiasi informazione che consenta di risalire all'identita del cliente

CONSENTITO con consapevolezza:

- Ricerca normativa e giurisprudenziale generale (verificare sempre le fonti)
- Bozze di testi su casi anonimi o ipotetici
- Sintesi di testi pubblici, dottrina, legislazione
- Revisione grammaticale e formale di testi anonimi

OBBLIGATORIO in ogni caso:

- Verificare ogni citazione normativa o giurisprudenziale prodotta dall'AI
- Non firmare atti basati su output AI senza revisione critica approfondita
- Dichiarare l'uso dell'AI al cliente ove richiesto o rilevante

Strumenti AI con maggiore riservatezza

Strumento	Privacy	Note per uso legale
Modello locale (Ollama+LLaMA)	Massima	Gira sul PC dello studio; nessun dato esce; richiede hardware adeguato
Claude for Enterprise	Alta	Anthropic: no training su dati enterprise; DPA disponibile
ChatGPT Enterprise	Alta	OpenAI: no training su dati enterprise; audit log disponibile
ChatGPT / Claude (piano gratuito)	Bassa	I dati possono essere usati per training. Non usare per dati riservati.

7. Autenticazione Avanzata e Segregazione del Dispositivo

7.1 Architettura 2FA Completa per lo Studio

Non basta attivare il 2FA: occorre farlo in modo coerente, su tutti i servizi critici, con metodi sicuri e con un piano di recupero documentato.

Servizio	Metodo 2FA minimo	Metodo raccomandato
Email professionale	TOTP (app authenticator)	FIDO2 / YubiKey
Password manager	TOTP	FIDO2 + TOTP come backup
Cloud documenti	TOTP	FIDO2
Gestionale dello studio	TOTP	SSO con MFA centralizzato
Accesso VPN	Certificato + password	Certificato + TOTP
Portali PA / SPID	SPID L2 (include gia 2FA)	SPID L2 con app dedicata
Home banking studio	Token OTP hardware (banca)	Token OTP hardware dedicato

7.2 Chiavi Hardware FIDO2

Le chiavi hardware FIDO2/WebAuthn sono il metodo di autenticazione piu sicuro disponibile al pubblico. Resistono agli attacchi di phishing perche la risposta crittografica dipende dal dominio del sito: una chiave rubata non funziona su siti falsi.

- Acquistare sempre almeno 2 chiavi (una primaria, una di backup)
- Registrare entrambe le chiavi su ogni servizio critico al momento dell'attivazione
- Conservare la chiave di backup in luogo fisico sicuro (cassaforte, cassetto blindato)
- Non collegare la chiave al computer quando non e necessario
- Costo indicativo: 50-90 euro per chiave (YubiKey 5 Series, Nitrokey)

7.3 Gestione dei Codici di Backup 2FA

Procedura obbligatoria: Codici di recupero 2FA

Ogni servizio con 2FA attivo genera codici di recupero monouso. Procedura:

1. Generare i codici al momento dell'attivazione del 2FA
2. Stampare e archiviare fisicamente in cassaforte o luogo dedicato sicuro
3. In alternativa: cifrare con VeraCrypt e archiviare su due supporti separati
4. NON salvare i codici sullo stesso dispositivo usato per il 2FA
5. Documentare chiaramente a quale account corrisponde ogni set di codici

6. Rigenerare i codici se si sospetta che qualcuno li abbia visti

Perdere l'accesso al 2FA senza codici di backup significa perdere l'accesso all'account. Questa situazione, in ambito professionale, puo avere conseguenze operative gravi.

7.4 Modello di Segregazione Completa del Dispositivo Mobile

Elemento	Telefono Professionale	Telefono Personale
Numero SIM	Numero professionale (comunicato ai clienti)	Numero privato
Account email	Solo account professionali	Solo account personali
App installate	Email, VPN, authenticator, documenti, telefonia	Social, gaming, streaming, banking personale
App authenticator	Account professionali (email, cloud, gestionale)	Account personali
WhatsApp	NON installato	Solo uso personale; mai dati clienti
Backup	Gestito dallo studio, cifrato	Personale (iCloud, Google)
Cancellazione remota	Studio puo cancellare tramite MDM	Gestita personalmente

8. Risposta agli Incidenti

Nessuna misura e infallibile al 100%. La capacita di rispondere rapidamente e correttamente a un incidente e parte integrante del protocollo di sicurezza.

8.1 Classificazione degli Incidenti

Livello	Esempi	Azione richiesta
CRITICO	Ransomware, breach confermato, accesso non autorizzato a dati clienti	Isolamento immediato, notifica Garante entro 72h, notifica clienti, supporto legale
ALTO	Account compromesso, phishing andato a buon fine, dispositivo perso	Cambio credenziali immediato, revoca sessioni, analisi impatto
MEDIO	Email sospette, tentativo di accesso bloccato	Documentazione, monitoraggio, revisione misure preventive
BASSO	Spam anomalo, errori di sistema isolati	Log e monitoraggio; nessuna azione immediata

8.2 Procedura di Risposta a un Incidente Critico

1. CONTENIMENTO (entro 1 ora): Disconnettere il dispositivo compromesso dalla rete. Non spegnerlo immediatamente: la memoria volatile contiene informazioni preziose per l'analisi forense.
2. VALUTAZIONE (entro 4 ore): Identificare quali dati sono stati esposti. Coinvolgere un esperto di incident response se lo studio non ha competenze tecniche interne.
3. NOTIFICA INTERNA (entro 4 ore): Informare tutti i membri dello studio. Cambiare le credenziali di tutti gli account potenzialmente accessibili dal dispositivo compromesso.
4. NOTIFICA AL GARANTE (entro 72 ore): Se il breach riguarda dati personali, notifica obbligatoria al Garante Privacy tramite portale gpdp.it. Obbligo di legge GDPR art. 33.
5. NOTIFICA AI CLIENTI (valutare): Se i dati dei clienti sono stati esposti e il rischio e elevato, informarli senza ingiustificato ritardo. GDPR art. 34.
6. DOCUMENTAZIONE: Registrare cronologicamente ogni azione intrapresa. Fondamentale sia per il Garante che per eventuali procedure legali.
7. RIPRISTINO: Ripristinare i sistemi da backup pulito verificato. Non ripristinare da backup potenzialmente compromesso.
8. POST-INCIDENT REVIEW: Analizzare come e avvenuto l'incidente. Aggiornare questo protocollo per prevenire recidive.

Contatti di emergenza: preparare PRIMA dell'incidente

- Esperto di incident response / consulente IT di fiducia: [inserire numero]

- Portale notifiche Garante Privacy: gpdp.it/it/web/guest/home
- Polizza assicurativa cyber (se disponibile): numero sinistri [inserire]
- Provider hosting / cloud: numero supporto di emergenza
- Fornitore antivirus / EDR: numero escalation

Stampare questo elenco e conservarlo fisicamente in un luogo accessibile anche senza rete.

9. Formazione del Personale e Cultura della Sicurezza

Il fattore umano e la causa principale degli incidenti informatici. Le misure tecniche proteggono solo se le persone sanno come comportarsi. La formazione non e un costo accessorio: e una misura di sicurezza fondamentale.

9.1 Piano di Formazione Minimo

Argomento	Frequenza	Contenuto chiave
Phishing e social engineering	Annuale + simulazioni	Riconoscere attacchi, procedura di segnalazione, casi reali
Password e 2FA	Onboarding + annuale	Uso del password manager, configurazione 2FA, gestione backup
Gestione documenti e cloud	Onboarding	Dove archiviare, cosa non condividere, classificazione
Uso responsabile dell'AI	All'introduzione dello strumento	Cosa inserire, cosa vietare, come verificare output
Risposta agli incidenti	Annuale	Cosa fare nelle prime ore, chi chiamare, cosa NON fare

9.2 Le 10 Regole d'Oro

Promemoria operativo: le 10 regole d'oro della sicurezza informatica per avvocati

1. Password unica e lunga per ogni account. Mai riusare.
2. 2FA attivo su tutti i servizi critici. Mai via SMS se possibile.
3. Aggiornare sempre il sistema operativo e le applicazioni.
4. Non aprire allegati o link sospetti. In dubbio, chiamare il mittente.
5. Usare VPN su qualsiasi rete diversa da quella dell'ufficio.
6. Non inserire dati identificativi dei clienti in AI cloud.
7. Cifrare i dispositivi e bloccarli quando non in uso.
8. Fare backup regolari e verificarne il funzionamento reale.
9. Segnalare immediatamente qualsiasi anomalia al responsabile.
10. Il dubbio e una misura di sicurezza: se qualcosa sembra strano, lo e.

10. Checklist di Implementazione per Priorita

Le misure di sicurezza vanno introdotte in ordine di priorita. Questa checklist e progettata per essere stampata e usata operativamente. Spuntare ogni voce solo dopo aver verificato l effettiva implementazione.

Come usare questa checklist

Priorita 1 (entro 30 giorni): misure essenziali a costo zero o minimo, massimo impatto immediato.

Priorita 2 (entro 90 giorni): misure strutturali che richiedono qualche configurazione o acquisto.

Priorita 3 (entro 6 mesi): misure avanzate per uno studio maturo nella sicurezza.

Ogni voce include la verifica da effettuare prima di spuntarla.

Conservare copia firmata come documentazione per eventuali audit GDPR.

Priorita 1 — Azioni immediate (entro 30 giorni)

	Azione	Come verificare	Completato
[ ]	Installare password manager (Bitwarden o 1Password) e creare la Master Password	Aprire il vault e generare la prima password	Data: _____
[ ]	Annotare la Master Password su carta e conservarla in cassaforte	Copia cartacea esiste in luogo fisicamente sicuro	Data: _____
[ ]	Attivare 2FA sull account email professionale con app TOTP (Aegis, Authy) — NON via SMS	Testare login con 2FA su dispositivo diverso	Data: _____
[ ]	Salvare i codici di recupero 2FA stampati, separati dal dispositivo	Codici stampati e conservati in luogo sicuro separato	Data: _____
[ ]	Verificare PIN alfanumerico minimo 8 caratteri su tutti i dispositivi	Testare blocco schermo su ogni dispositivo	Data: _____
[ ]	Abilitare aggiornamenti automatici del sistema operativo su tutti i dispositivi	Aggiornamenti automatici attivi nelle impostazioni	Data: _____
[ ]	Mappare dove risiedono i dati dei clienti e verificare che l accesso sia protetto	Lista scritta dei depositi dati con relativa protezione	Data: _____
[ ]	Comunicare al team: nessun dato identificativo dei clienti in strumenti AI cloud	Comunicazione scritta ricevuta da tutti i membri	Data: _____

Priorita 2 — Azioni strutturali (entro 90 giorni)

	Azione	Come verificare	Completato
[ ]	Attivare 2FA su tutti i servizi cloud, gestionali e portali istituzionali	Lista completa servizi con 2FA abilitato	Data: _____
[ ]	Richiedere e firmare il DPA con il provider cloud (obbligatorio GDPR)	Copia firmata del DPA archiviata	Data: _____
[ ]	Implementare backup 3-2-1: 3 copie, 2 supporti diversi, 1 off-site	Schema backup documentato e automatizzato	Data: _____
[ ]	Eseguire primo test di ripristino dal backup — file effettivamente recuperabili	File ripristinato con successo, esito documentato	Data: _____
[ ]	Installare e configurare VPN per il lavoro remoto	VPN testata da postazione remota su dati reali	Data: _____
[ ]	Migrare tutte le credenziali nel password manager con password uniche per ogni servizio	Nessuna password ripetuta nei servizi critici	Data: _____
[ ]	Formare il team sul riconoscimento del phishing con simulazione pratica	Sessione completata, partecipanti documentati	Data: _____
[ ]	Definire e distribuire la politica di utilizzo accettabile (AUP) firmata da tutto il team	Documento firmato da tutti i membri del team	Data: _____

Priorita 3 — Azioni avanzate (entro 6 mesi)

	Azione	Come verificare	Completato
[ ]	Attivare cifratura disco su tutti i PC (BitLocker su Windows, FileVault su Mac)	Cifratura attiva verificata nelle impostazioni	Data: _____
[ ]	Configurare SPF, DKIM e DMARC sul dominio email dello studio	Test su mxtoolbox.com con risultato PASS	Data: _____
[ ]	Valutare e implementare sistema MDM per la gestione centralizzata dei dispositivi mobili	Tutti i dispositivi mobili registrati nel MDM	Data: _____
[ ]	Adottare strumento di comunicazione cifrata per clienti (Signal + ProtonMail)	Strumento operativo e comunicato ai	Data: _____

		clienti	
[ ]	Formalizzare politica di uso dell AI con procedura di anonimizzazione e strumenti approvati	Documento firmato da tutti i membri del team	Data: _____
[ ]	Condurre simulazione tabletop di risposta a incidente (ransomware, phishing, device smarrito)	Simulazione effettuata, lezioni apprese documentate	Data: _____
[ ]	Verificare e aggiornare il registro dei trattamenti GDPR	Registro completo, aggiornato e archiviato	Data: _____
[ ]	Valutare chiavi hardware YubiKey per titolari e ruoli con accesso ai dati piu sensibili	Chiavi configurate e testate su account critici	Data: _____

Responsabile: _____ Data ultima revisione: _____

11. Appendice: Risorse e Riferimenti

11.1 Fonti Normative

- GDPR: eur-lex.europa.eu (Regolamento UE 2016/679)
- Codice Privacy IT: normattiva.it (D.Lgs. 196/2003)
- Codice Deontologico Forense: cnf.it
- Garante Privacy Italia - notifiche breach: gpdp.it
- NIS2: eur-lex.europa.eu (Direttiva UE 2022/2555)

11.2 Risorse Tecniche

- NIST Cybersecurity Framework: nist.gov/cyberframework
- NIST SP 800-63B (politica password): pages.nist.gov/800-63-3
- ENISA - Agenzia UE per la Cybersicurezza: enisa.europa.eu
- Have I Been Pwned - verifica account compromessi: haveibeenpwned.com

11.3 Strumenti Open Source Citati

- Bitwarden - password manager: bitwarden.com
- KeePassXC - password manager locale: keepassxc.org
- Aegis Authenticator - 2FA Android: getaegis.app
- Signal - messaggistica cifrata: signal.org
- VeraCrypt - cifratura file e disco: veracrypt.fr
- ProtonMail / ProtonDrive - email e cloud cifrati: proton.me
- Nextcloud - cloud privato: nextcloud.com
- Ollama - AI locale: ollama.ai

11.4 Log delle Revisioni

Versione	Data	Note
1.0	2025	Prima pubblicazione. Centuria Foundation - centuriafoundation.pl

Centuria Foundation

centuriafoundation.pl