€

PROTOCOLLO DI CYBERSECURITY

PER COMMERCIALISTI E STUDI FISCALI

Protezione di dati fiscali, accessi istituzionali, fatturazione elettronica e intelligenza artificiale

Applicabile a commercialisti singoli, associati e studi fiscali di ogni dimensione

Centuria Foundation
centuriafoundation.pl
Versione 1.0 | 2025

Indice

1. Introduzione e Contesto Normativo

I commercialisti e gli studi fiscali gestiscono alcune delle informazioni piu critiche per persone e imprese: dichiarazioni dei redditi, bilanci, situazioni patrimoniali, accessi all Agenzia delle Entrate, credenziali di fatturazione elettronica, deleghe fiscali. Un attacco informatico a uno studio commerciale non colpisce solo il professionista: colpisce direttamente i clienti, esponendo dati finanziari riservati, consentendo frodi fiscali e potenzialmente azzerando anni di archivi contabili.

Il rischio e amplificato dal fatto che i commercialisti operano come intermediari fiscali abilitati con accesso diretto ai sistemi dell Agenzia delle Entrate, al Cassetto Fiscale dei clienti, ai portali INPS, alle Camere di Commercio. Le credenziali di un commercialista compromesse valgono molto di piu di quelle di un privato cittadino.

1.1 Riferimenti Normativi

Norma / Regolamento	Rilevanza per il Commercialista
GDPR (Reg. UE 2016/679)	Protezione dei dati personali dei clienti (persone fisiche). Misure tecniche adeguate obbligatorie. Notifica breach entro 72 ore al Garante.
D.Lgs. 196/2003 (Codice Privacy)	Base normativa italiana. Obbligo di misure di sicurezza per chi tratta dati personali in ambito professionale.
D.Lgs. 231/2007 (Antiriciclaggio)	Obbligo di conservazione sicura delle informazioni AML. Adeguata verifica della clientela con dati sensibili.
Codice Deontologico CNDCEC	Obbligo di riservatezza professionale sulle informazioni acquisite nell esercizio della professione.
D.Lgs. 82/2005 (CAD)	Codice dell Amministrazione Digitale: regole per la gestione dei documenti informatici e delle firme digitali.
NIS2 (Dir. UE 2022/2555)	Studi con oltre 50 dipendenti o che gestiscono infrastrutture critiche rientrano nell ambito.
D.Lgs. 231/2001	Responsabilita amministrativa degli enti. La mancanza di misure di sicurezza adeguate puo configurare colpa organizzativa.

Il Commercialista come Bersaglio Prioritario

I criminali informatici prendono di mira gli studi commerciali perche:

- Le credenziali dell intermediario fiscale danno accesso ai conti di TUTTI i clienti
- I dati finanziari permettono frodi fiscali, accessi bancari, furto d identita
- Gli archivi contabili sono critici per la continuita operativa dei clienti imprese
- I pagamenti di imposte e contributi possono essere dirottati su conti terzi
- Le deleghe bancarie e i poteri di firma sono informazioni di estremo valore

Un singolo attacco andato a buon fine puo compromettere decine o centinaia di clienti.

2. Gestione delle Credenziali Istituzionali

La categoria di rischio piu critica per un commercialista e la compromissione delle credenziali istituzionali: SPID professionale, Entratel, Fisconline, portali INPS, Camere di Commercio, PEC. Queste credenziali hanno un valore straordinariamente alto per i criminali informatici.

2.1 Mappa delle Credenziali Critiche

Sistema	Accesso consente	Livello di rischio
Entratel / Fisconline	Dichiarazioni fiscali di tutti i clienti deleganti, F24, rimborsi	CRITICO
Cassetto Fiscale clienti	Visura completa situazione fiscale, atti, avvisi bonari	CRITICO
SPID professionale	Accesso a tutti i servizi PA con identita digitale certificata	CRITICO
Portale INPS intermediari	Dati previdenziali e contributivi di tutti i clienti	MOLTO ALTO
Registro Imprese / CCIAA	Visure, atti societari, poteri di firma	MOLTO ALTO
PEC professionale	Comunicazioni ufficiali, notifiche, atti giudiziari	ALTO
Software gestionale	Archivio contabile completo di tutti i clienti	CRITICO
Home banking deleghe	Accesso ai conti correnti dei clienti con delega	CRITICO

2.2 Regole Operative per le Credenziali Istituzionali

Regole non negoziabili per le credenziali istituzionali

1. Le credenziali Entratel / SPID / INPS non si condividono mai con nessuno, inclusi collaboratori dello studio. Ogni professionista deve avere le proprie.

2. Non salvare mai le credenziali istituzionali nel browser (Chrome, Firefox, Safari). Usare esclusivamente il password manager dello studio.

3. Attivare il 2FA su tutti i sistemi istituzionali che lo supportano. Alcuni portali AgE lo impongono gia: verificare lo stato su tutti gli accessi.

4. In caso di sospetta compromissione: modificare immediatamente le credenziali E contattare il supporto del sistema interessato (es. Entratel: 800.90.96.96).

5. Non accedere ai sistemi istituzionali da dispositivi non dello studio (PC di clienti, computer pubblici, dispositivi personali non protetti).

2.3 Password Policy per Credenziali Professionali

Parametro	Requisito
Lunghezza minima	20 caratteri per credenziali istituzionali (Entratel, SPID, INPS). 16 per gli altri sistemi.
Composizione	Lettere maiuscole/minuscole, numeri, simboli. Mai parole di dizionario o riferimenti al codice fiscale.
Unicita assoluta	Password diversa per ogni portale istituzionale e per ogni cliente. Zero eccezioni.
Rotazione	Cambio ogni 6 mesi per credenziali istituzionali. 12 mesi per gli altri sistemi. Immediato se compromissione sospetta.
Gestione team	Ogni collaboratore con accesso delegato deve avere proprie credenziali: mai condivise.

3. Password Manager e Autenticazione a Due Fattori

3.1 Password Manager: Obbligatorio

Uno studio commerciale gestisce decine se non centinaia di accessi diversi: un portale per ogni cliente, piu portali istituzionali, software gestionali, email, cloud. Gestire tutto questo senza un password manager significa inevitabilmente riutilizzare le password, con conseguenze catastrofiche in caso di breach.

Strumento	Caratteristiche	Livello
Bitwarden Business	Open source, cloud EU, gestione team con permessi granulari, audit log. Piano business economico.	Consigliato
1Password Teams	Vault condivisi per team, integrazione SSO, report di sicurezza automatici.	Professionale
KeePassXC + sincronizzazione	File locale cifrato sincronizzato su cloud privato (Nextcloud). Massimo controllo.	Avanzato

3.2 Autenticazione a Due Fattori: Priorita per lo Studio Fiscale

Per uno studio commerciale il 2FA non e una raccomandazione: e una necessita operativa. Le credenziali fiscali compromesse senza 2FA permettono accesso immediato a dichiarazioni, rimborsi e dati di tutti i clienti.

Metodo	Applicabilita in ambito fiscale	Livello
App TOTP (Aegis, Authy)	Supportato dalla maggior parte dei portali istituzionali italiani. Codice ogni 30 secondi offline.	Molto alto - usare
SPID con livello 2	SPID livello 2 gia incorpora 2FA. Verificare che tutti gli accessi usino SPID L2, non L1.	Molto alto - usare
Chiave hardware (YubiKey)	Massima sicurezza. Supportato da portali europei e internazionali.	Massimo - consigliato
SMS	Vulnerabile. Usare solo dove non esiste alternativa (alcuni portali AgE legacy).	Evitare se possibile

3.3 Sistemi su cui Attivare il 2FA Immediatamente

- Email professionale (PEC e email ordinaria)
- Entratel e Fisconline
- SPID professionale (verificare livello 2)
- Portale INPS intermediari
- Software gestionale contabile
- Cloud storage con documenti clienti
- Home banking con deleghe clienti
- Password manager
- VPN dello studio

4. Fatturazione Elettronica, SDI e Firma Digitale

La fatturazione elettronica obbligatoria e il Sistema di Interscambio (SDI) dell Agenzia delle Entrate introducono rischi specifici che vanno gestiti con attenzione. La firma digitale e il sigillo informatico sono strumenti di altissimo valore che devono essere protetti adeguatamente.

4.1 Sicurezza del Sistema di Fatturazione Elettronica

Rischio specifico	Misura di protezione
Credenziali portale fatturazione	Usare password unica e forte. Attivare 2FA se disponibile. Mai salvare nel browser.
Accesso SDI tramite intermediario	Verificare periodicamente le deleghe attive: revocare quelle non necessarie o di ex collaboratori.
Intercettazione fatture	Le fatture contengono dati fiscali sensibili. Archiviare solo su cloud cifrato con accesso controllato.
Manipolazione IBAN su fatture	Verificare telefonicamente con il cliente qualsiasi variazione di IBAN comunicata via email.
Malware su PC di fatturazione	PC usato per la fatturazione elettronica deve avere antivirus attivo e aggiornato. Nessun uso personale.

Attenzione: Frode IBAN (CEO Fraud e BEC)

Una delle frodi piu diffuse negli studi commerciali e la sostituzione dell IBAN: un criminale intercetta una comunicazione, modifica il numero di conto e reindirizza il pagamento su un conto fraudolento.

Regola operativa obbligatoria:

- Qualsiasi variazione di IBAN comunicata via email o messaggio deve essere SEMPRE verificata telefonicamente con il cliente o il fornitore chiamando un numero gia noto, mai quello indicato nella email sospetta.

- Questa regola vale anche se l email sembra provenire da un contatto fidato: le email possono essere spoofate o l account del mittente puo essere stato compromesso.

4.2 Firma Digitale e CNS: Protezione del Dispositivo

La firma digitale e la Carta Nazionale dei Servizi (CNS) sono strumenti di identificazione e firma con valore legale. La loro compromissione permette di firmare documenti, atti e dichiarazioni a nome del professionista.

- Il PIN della firma digitale non va mai scritto su carta insieme al dispositivo fisico
- I dispositivi di firma (smart card, token USB) vanno conservati in luogo sicuro quando non in uso
- Non lasciare il token di firma inserito nel PC incustodito: rimuoverlo dopo ogni utilizzo
- In caso di smarrimento o furto del dispositivo di firma: revoca immediata presso l ente certificatore

- Verificare periodicamente la scadenza dei certificati: rinnovo tempestivo evita interruzioni operative
- Non delegare mai la firma digitale a collaboratori: e un atto personale e intrasferibile

5. Email, PEC e Comunicazioni con i Clienti

Le comunicazioni dello studio commerciale contengono dati finanziari, fiscali e patrimoniali di altissimo valore. La PEC ha valore legale di raccomandata con ricevuta di ritorno: la sua sicurezza e sia un obbligo deontologico che una necessita pratica.

5.1 PEC: Regole di Sicurezza Specifiche

La PEC non e automaticamente sicura

La PEC garantisce la consegna certificata e il valore legale del messaggio,
ma NON garantisce la cifratura del contenuto durante il transito.

Misure obbligatorie per la PEC professionale:

- Password PEC unica e forte, cambiata ogni 6 mesi
- 2FA attivo sull account PEC (la maggior parte dei provider lo supporta)
- Accesso PEC solo da dispositivi professionali protetti
- Archivio PEC su sistema cifrato: i messaggi contengono atti e documenti legali
- Non aprire allegati PEC sospetti: anche la PEC puo essere vettore di malware
- Verificare il mittente: la PEC garantisce il gestore, non l identita del mittente reale

5.2 Email Professionale Ordinaria

Misura	Dettaglio
Dominio proprietario	Usare @nomestudio.it. Mai Gmail o Hotmail personale per comunicazioni professionali con clienti.
SPF, DKIM, DMARC	Record DNS contro spoofing del dominio. Essenziale per uno studio che gestisce dati fiscali.
2FA sull account	Obbligatorio. Vedi Sezione 3.
Cifratura TLS	Verifica che il provider supporti TLS 1.2+. La maggior parte dei provider professionali lo fa.
Archivio cifrato	Email con dati fiscali archiviate su storage cifrato.

5.3 Comunicazione di Dati Fiscali ai Clienti

L invio di documenti fiscali (dichiarazioni, F24, bilanci, CU) via email standard non e sicuro. I dati finanziari dei clienti meritano un canale protetto.

Strumento	Caratteristiche	Uso consigliato
Portale clienti con accesso autenticato	Area riservata per ogni cliente con login. Massima professionalita e sicurezza.	Studi strutturati
Email cifrata (ProtonMail, S/MIME)	Cifratura end-to-end. Richiede che anche il cliente usi un client compatibile.	Clienti tecnici
Piattaforma di document sharing	Condivisione con link protetto da password e scadenza. GDPR	Tutti i clienti

sicura (Tresorit, SharePoint)	compliant.	
PEC del cliente	Valore legale, consegna certificata. Per atti ufficiali e scadenze formali.	Comunicazioni ufficiali

6. Software Gestionale e Archivio Contabile

Il software gestionale contabile e il patrimonio informativo piu critico di uno studio: contiene bilanci, dichiarazioni, registri IVA, libri contabili e dati finanziari di tutti i clienti. Un attacco ransomware su questo sistema e potenzialmente devastante.

6.1 Requisiti di Sicurezza per il Software Gestionale

Requisito	Dettaglio e Verifica
Cifratura del database	I dati contabili devono essere cifrati at-rest. Chiedere conferma scritta al fornitore del software.
Log di accesso	Registro automatico di chi ha acceduto a quali dati e quando. Essenziale per GDPR e audit.
Aggiornamenti di sicurezza	Il fornitore deve rilasciare patch di sicurezza tempestive. Applicarle entro 72 ore dal rilascio.
DPA con il fornitore	Il fornitore del gestionale tratta dati personali dei vostri clienti: DPA obbligatorio ex GDPR.
Backup automatico	Backup giornaliero automatico su supporto separato. Verifica mensile di integrita.
Accesso remoto	Se il gestionale e accessibile da remoto: solo tramite VPN o accesso cifrato certificato.
Autenticazione	Il gestionale deve supportare credenziali individuali per ogni operatore. Niente account condivisi.

6.2 Struttura degli Accessi nel Software Gestionale

In uno studio con piu collaboratori e fondamentale che gli accessi al gestionale siano strutturati per ruolo. Non tutti devono poter vedere i dati di tutti i clienti.

Ruolo	Accesso consigliato	Restrizioni
Titolare / Socio	Accesso completo a tutti i clienti e funzioni	Nessuna
Collaboratore senior	Accesso ai clienti assegnati, funzioni operative complete	Solo clienti assegnati
Praticante / Collaboratore junior	Accesso ai clienti assegnati, senza funzioni di firma o invio	Solo clienti assegnati, sola lettura su altri
Segreteria / Amministrativo	Dati anagrafici, scadenzario, fatturazione studio	Nessun accesso dati contabili clienti
Consulente esterno	Accesso temporaneo al singolo cliente, revocato al termine	Accesso limitato nel tempo

6.3 Protezione Anti-Ransomware

Il ransomware e la minaccia principale per gli studi commerciali: cifra tutti i file e chiede riscatto. La protezione non e solo tecnologica: e procedurale.

- Backup offline: almeno una copia dei dati deve essere su supporto non connesso alla rete (disco esterno disconnesso, nastro)
- Backup immutabile: usare storage cloud con versioning abilitato (OneDrive, Tresorit) — il ransomware non puo cancellare le versioni precedenti
- Segmentazione di rete: il server del gestionale non deve essere sulla stessa rete dei PC usati per navigazione
- Principio del minimo privilegio: i collaboratori non devono avere diritti di amministratore sui propri PC
- Blocco esecuzione macro: disabilitare l esecuzione automatica di macro in Word ed Excel — vettore primario di infezione

7. Cloud, Archiviazione e Strategia di Backup

I dati fiscali e contabili hanno obblighi di conservazione legali precisi. La strategia di archiviazione deve bilanciare accessibilita, sicurezza e conformita normativa.

7.1 Criteri di Scelta del Cloud per Dati Fiscali

Criterio	Requisito specifico per dati fiscali
Server in UE	Obbligatorio per GDPR. I dati fiscali non possono risiedere su server extraeuropei senza garanzie specifiche.
Cifratura AES-256	At-rest e in-transit. Preferibile cifratura lato client per i documenti piu sensibili.
DPA solido	Il provider diventa responsabile del trattamento ex GDPR: DPA specifico obbligatorio.
Versioning dei file	Obbligatorio per protezione anti-ransomware: capacita di ripristinare versioni precedenti dei documenti.
Audit log	Log di accesso ai file con esportazione per audit Garante o controlli dell Agenzia delle Entrate.
SLA di disponibilita	Minimo 99.9% uptime garantito: gli studi commerciali hanno scadenze fiscali inderogabili.

Provider valutati per studi fiscali

Provider	Note per uso fiscale	Valutazione
Microsoft 365 Business	SharePoint per gestione documentale, server EU, DPA, versioning nativo, integrazione Teams.	Raccomandato
Tresorit	Cifratura end-to-end lato client, server UE, DPA solido. Eccellente per studi piccoli.	Consigliato
Nextcloud (self-hosted o hosted EU)	Controllo totale, nessuna dipendenza da terze parti, versioning. Richiede competenza tecnica.	Avanzato
Google Workspace Business	DPA disponibile, server EU con configurazione. Verificare impostazioni privacy con attenzione.	Con cautela

7.2 Obblighi di Conservazione dei Documenti Fiscali

Retention obbligatoria per documenti fiscali (riferimento normativo italiano)

Registri contabili (IVA, giornale, inventari): 10 anni dall ultima registrazione (art. 2220 c.c.)

Dichiarazioni fiscali e relative documentazione: 5 anni dalla presentazione (art. 43 DPR 600/73)

Documenti per accertamento: fino alla scadenza del termine di accertamento (5 anni)

Fatture elettroniche: 10 anni (art. 2220 c.c.)

Libri societari: illimitata per le societa in attivita

I backup devono rispettare questi termini di conservazione.
I dati non possono essere cancellati prima della scadenza del termine di legge,
anche in caso di fine del rapporto professionale con il cliente.

7.3 Strategia di Backup per lo Studio Fiscale

Regola 3-2-1 applicata ai Dati Fiscali

3 copie dei dati (originale + 2 backup)
2 supporti diversi (es. server locale cifrato + cloud EU con versioning)
1 copia offline fisicamente separata (disco esterno non connesso, conservato fuori sede)

Frequenza raccomandata:
- Backup incrementale automatico: ogni giorno (dopo chiusura dello studio)
- Backup completo: settimanale
- Backup offline su disco esterno: mensile, conservato fuori sede
- Test di ripristino: ogni 3 mesi con verifica dell integrita dei dati

Prima delle scadenze fiscali principali (31/3, 30/6, 30/9, 31/10):
eseguire un backup manuale aggiuntivo e verificarne il funzionamento.

8. Dispositivi, Reti e Lavoro da Remoto

I commercialisti lavorano sempre piu spesso in mobilita: visite ai clienti, lavoro da casa, accessi da tablet. Ogni accesso remoto ai sistemi dello studio e un potenziale punto di vulnerabilita se non gestito correttamente.

8.1 Configurazione Minima dei Dispositivi

Misura	Dettaglio
Cifratura disco	BitLocker (Windows) o FileVault (Mac) su tutti i PC. Obbligatorio per chi porta il laptop fuori sede.
PIN / password dispositivo	Minimo 8 caratteri alfanumerici. Blocco automatico entro 5 minuti di inattivita.
Antivirus aggiornato	Soluzione antivirus attiva con aggiornamento automatico delle firme virali.
Aggiornamenti OS	Aggiornamenti automatici abilitati. Nessun sistema operativo fuori supporto.
Separazione uso	I PC dello studio non vengono usati per navigazione personale o download non professionali.
Screen privacy filter	Per chi lavora in mobilita: filtro privacy sullo schermo per impedire shoulder surfing.

8.2 VPN: Obbligatoria per Accessi Remoti

Qualsiasi accesso ai sistemi dello studio (gestionale, cloud, email) da fuori sede deve avvenire tramite VPN. Il lavoro da casa o dal cliente non puo avvenire senza questa protezione.

- VPN aziendale (WireGuard, OpenVPN) o servizio business: mai VPN gratuite
- La VPN deve essere attiva prima di accedere a Entratel, gestionale, cloud studio
- Provider raccomandati con no-log policy verificata: ProtonVPN Business, Mullvad for Teams
- Configurare il kill switch VPN: se la VPN cade, bloccare tutto il traffico automaticamente

8.3 Policy BYOD per lo Studio Fiscale

Regole per Dispositivi Personali (BYOD)

Se si usano dispositivi personali per accedere ai sistemi dello studio:

- Il dispositivo deve soddisfare i requisiti minimi di sicurezza (sezione 8.1)
- Installare un profilo MDM separato per i dati professionali
- I documenti fiscali dei clienti non devono mai essere salvati nella memoria personale
- In caso di smarrimento o furto: segnalazione immediata per attivare cancellazione remota
- Fine rapporto lavorativo: cancellazione certificata di tutti i dati dello studio dal dispositivo

Raccomandazione forte: dispositivi dedicati allo studio evitano il 90% dei rischi BYOD.
Il costo di un laptop professionale e infinitamente inferiore al costo di un breach.

9. Uso dell Intelligenza Artificiale in Ambito Fiscale

L AI generativa offre potenziale significativo per i commercialisti: redazione di lettere al cliente, analisi di normativa fiscale, sintesi di circolari, preparazione di report. I rischi per la riservatezza dei dati fiscali dei clienti richiedono pero un protocollo esplicito.

9.1 Rischi Specifici in Ambito Fiscale

I dati fiscali sono dati personali ai sensi del GDPR. Inserire redditi, patrimoni, situazioni debitorie o informazioni societarie di un cliente in un sistema AI cloud senza consenso specifico e una violazione del GDPR e del dovere di riservatezza professionale.

Regola Fondamentale: AI e Dati Fiscali dei Clienti

Non inserire MAI in sistemi AI generativi cloud:

- Codice fiscale, partita IVA, dati anagrafici del cliente
- Redditi, patrimoni, situazioni debitorie o creditorie
- Contenuto di dichiarazioni fiscali, bilanci, registri contabili
- Informazioni su contenziosi fiscali, avvisi bonari, accertamenti
- Dati societari riservati (soci occulti, strutture di controllo, patti parasociali)
- Qualsiasi dato che consenta di risalire all identita e alla situazione del cliente

L AI puo essere usata per:

- Ricerca e analisi di normativa fiscale pubblica (circolari, risoluzioni, prassi AgE)
- Bozze generiche di lettere o comunicazioni su fattispecie anonime
- Sintesi di documenti normativi pubblici
- Preparazione di template e format anonimi

9.2 Strumenti AI Valutati per Uso Fiscale

Strumento	Note per uso fiscale	Valutazione
LLM locali (Ollama, LM Studio)	Il modello gira sul dispositivo locale. Nessun dato esce. Ideale per dati sensibili.	Ottimo
Microsoft Copilot M365 Enterprise	Con piano Enterprise: dati non usati per training, DPA disponibile, server EU.	Accettabile in Enterprise
ChatGPT Enterprise / Claude API	Dati non usati per training con piano enterprise. Verificare termini aggiornati.	Accettabile con piano dedicato
ChatGPT / Gemini gratuiti	Dati possono essere usati per training. ASSOLUTAMENTE vietato per dati fiscali reali.	VIETATO

9.3 Procedura di Anonimizzazione

1. Sostituire nome/cognome con identificatori generici (es. Cliente X, Societa Alpha)
2. Rimuovere codice fiscale, partita IVA, indirizzo
3. Sostituire valori economici precisi con ordini di grandezza (es. 'circa 100.000 euro')
4. Rimuovere date specifiche di atti, accertamenti, contenziosi

5. Generalizzare il settore di attivita se identificante
6. Verificare che il testo anonimizzato non consenta la re-identificazione del cliente
7. Documentare l uso dello strumento AI nel registro delle attivita dello studio

10. Risposta agli Incidenti

In uno studio commerciale un incidente informatico puo avere conseguenze immediate: scadenze fiscali mancate, dati clienti esposti, accessi non autorizzati ai conti. Il piano va preparato prima che accada.

10.1 Classificazione degli Incidenti

Livello	Esempi in ambito fiscale	Azione immediata
CRITICO	Ransomware su gestionale, compromissione credenziali Entratel/SPID, data breach dati fiscali clienti	Isolare sistemi, cambiare credenziali istituzionali, notifica Garante entro 72h, informare clienti coinvolti
ALTO	Sospetto accesso non autorizzato a Entratel, phishing cliccato, dispositivo con dati fiscali smarrito	Cambiare tutte le credenziali, revocare sessioni, analizzare log di accesso, valutare notifica
MEDIO	Email sospetta ricevuta, tentativo di accesso bloccato, variazione IBAN sospetta	Documentare, verificare, applicare contromisure, informare il cliente se necessario

10.2 Piano di Continuita Operativa in Caso di Attacco

Business Continuity per lo Studio Fiscale

Le scadenze fiscali non aspettano. In caso di attacco informatico vicino a una scadenza:

1. Lista stampata delle scadenze imminenti (30 giorni) sempre disponibile offline
2. Backup cartaceo o offline dei dati dei clienti con scadenze critiche
3. Contatti diretti (telefono) di tutti i clienti con scadenze imminenti
4. Piano di accesso alternativo a Entratel / portali istituzionali
   (es. accesso da dispositivo di riserva non connesso alla rete studio)
5. Accordo con tecnico informatico di fiducia reperibile entro 4 ore

In caso di ransomware: NON PAGARE. Contattare immediatamente il CSIRT Italia.
Valutare la segnalazione alla Guardia di Finanza per reato informatico.

10.3 Procedura di Notifica Data Breach Dati Fiscali

8. CONTENIMENTO: Isolare immediatamente i sistemi coinvolti
9. VALUTAZIONE: Determinare quanti clienti sono coinvolti e quali dati esposti
10. NOTIFICA GARANTE: Obbligatoria entro 72 ore se dati personali di clienti sono esposti
11. NOTIFICA CLIENTI: Obbligatoria se il breach comporta rischio elevato per i diritti dei clienti
12. NOTIFICA ORDINE: Valutare segnalazione all Ordine dei Dottori Commercialisti ed Esperti Contabili
13. DOCUMENTAZIONE: Registro completo dell incidente con tutte le azioni intraprese
14. ANALISI CAUSE: Identificare la causa radice e rimuoverla
15. RIPRISTINO: Ripristinare da backup verificati e testati

Contatti Utili in Caso di Incidente

Garante Privacy - notifica breach: garanteprivacy.it/notifica-data-breach
CSIRT Italia (supporto tecnico): csirt.gov.it | Tel: 06 54 79 99 56
Polizia Postale (denuncia): commissariatodips.it
Supporto Entratel: 800.90.96.96 (gratuito da fisso)
Guardia di Finanza - reati informatici: gdf.gov.it

Conservare questi contatti stampati: in caso di ransomware i sistemi potrebbero non essere accessibili.

11. Checklist di Implementazione per Priorita

Checklist operativa progettata per essere stampata e usata. Spuntare ogni voce solo dopo verifica effettiva. Conservare copia firmata per audit GDPR e controlli dell Ordine.

Come usare questa checklist

Priorita 1 (entro 30 giorni): misure essenziali, massimo impatto immediato.
Priorita 2 (entro 90 giorni): misure strutturali che richiedono configurazione o acquisto.
Priorita 3 (entro 6 mesi): misure avanzate per uno studio maturo nella sicurezza.

Raccomandazione specifica per studi fiscali: eseguire Priorita 1 PRIMA della prossima scadenza fiscale principale.

Priorita 1 — Azioni immediate (entro 30 giorni)

	Azione	Come verificare	Completato
[ ]	Installare password manager e creare Master Password forte (non salvarla digitalmente)	Vault operativo, prima password generata con lo strumento	Data: _____
[ ]	Attivare 2FA su email professionale e PEC con app TOTP (non SMS)	Login 2FA testato da dispositivo diverso	Data: _____
[ ]	Attivare 2FA su Entratel / Fisconline e portale INPS intermediari	Accesso con 2FA testato su tutti i sistemi istituzionali	Data: _____
[ ]	Salvare codici di recupero 2FA stampati in cassaforte o armadio chiuso	Copia cartacea in luogo fisicamente sicuro	Data: _____
[ ]	Verificare che ogni collaboratore abbia credenziali individuali: vietati account condivisi	Lista utenti con credenziali individuali documentata	Data: _____
[ ]	Comunicare al team la regola anti-frode IBAN: verifica telefonica obbligatoria per ogni variazione	Regola scritta e firmata da tutti i collaboratori	Data: _____
[ ]	Abilitare aggiornamenti automatici OS su tutti i PC dello studio	Aggiornamenti automatici attivi su tutti i dispositivi	Data: _____
[ ]	Comunicare al team: nessun dato fiscale reale negli strumenti AI cloud gratuiti	Comunicazione scritta ricevuta da tutti i collaboratori	Data: _____

Priorita 2 — Azioni strutturali (entro 90 giorni)

	Azione	Come verificare	Completato

[ ]	Verificare e firmare il DPA con il fornitore del software gestionale	Copia firmata del DPA archiviata	Data: _____
[ ]	Implementare backup 3-2-1 con backup giornaliero automatico cifrato e copia offline mensile	Schema backup documentato, test ripristino eseguito	Data: _____
[ ]	Installare e configurare VPN per tutti gli accessi remoti ai sistemi dello studio	VPN testata da postazione remota su gestionale reale	Data: _____
[ ]	Migrare tutte le credenziali nel password manager con password uniche per ogni portale	Nessuna password ripetuta nei sistemi critici	Data: _____
[ ]	Attivare cifratura disco (BitLocker/FileVault) su tutti i PC, in particolare i portatili	Cifratura attiva e verificata su ogni dispositivo	Data: _____
[ ]	Configurare accessi al gestionale per ruolo: principio del minimo privilegio	Matrice accessi documentata e applicata nel software	Data: _____
[ ]	Formare il team su phishing, frode IBAN e uso sicuro delle credenziali istituzionali	Sessione completata, partecipanti documentati	Data: _____
[ ]	Disabilitare l esecuzione automatica di macro in Word ed Excel su tutti i PC	Impostazione macro verificata in ogni installazione Office	Data: _____

Priorita 3 — Azioni avanzate (entro 6 mesi)

	Azione	Come verificare	Completato
[ ]	Configurare SPF, DKIM e DMARC sul dominio email dello studio	Test su mxtoolbox.com con risultato PASS su tutti e tre	Data: _____
[ ]	Implementare sistema MDM per la gestione centralizzata dei dispositivi mobili	Tutti i dispositivi mobili professionali registrati nel MDM	Data: _____
[ ]	Valutare chiavi hardware YubiKey per i soci e i collaboratori con accesso a Entratel/SPID	Chiavi configurate e testate su tutti i sistemi istituzionali	Data: _____
[ ]	Formalizzare policy di uso dell AI con lista strumenti approvati e procedura anonimizzazione	Policy firmata da tutti i collaboratori	Data: _____
[ ]	Condurre simulazione tabletop di risposta a incidente (ransomware prima di una scadenza fiscale)	Simulazione completata, piano di continuita testato	Data: _____

[ ]	Implementare soluzione anti-ransomware con backup immutabile e versioning abilitato	Versioning attivo su cloud, backup offline testato	Data: _____
[ ]	Verificare e aggiornare il registro dei trattamenti GDPR con tutti i sistemi e fornitori	Registro completo, aggiornato, archiviato	Data: _____
[ ]	Valutare segmentazione di rete: server gestionale isolato dalla rete di navigazione	Segmentazione implementata e testata da tecnico	Data: _____

Responsabile sicurezza: _____ *Data ultima revisione:* _____

12. Appendice: Risorse e Riferimenti

12.1 Fonti Normative

- GDPR: eur-lex.europa.eu (Regolamento UE 2016/679)
- D.Lgs. 196/2003 (Codice Privacy): normattiva.it
- D.Lgs. 231/2007 (Antiriciclaggio): normattiva.it
- Garante Privacy - notifiche breach: garanteprivacy.it
- Codice Deontologico CNDCEC: cndcec.it
- NIS2: eur-lex.europa.eu (Direttiva UE 2022/2555)

12.2 Risorse Tecniche e Istituzionali

- CSIRT Italia: csirt.gov.it | Tel: 06 54 79 99 56
- NIST Cybersecurity Framework: nist.gov/cyberframework
- ENISA (Agenzia UE Cybersicurezza): enisa.europa.eu
- Supporto Entratel/Fisconline: 800.90.96.96
- Have I Been Pwned (verifica account compromessi): haveibeenpwned.com
- MXToolbox (test SPF/DKIM/DMARC): mxtoolbox.com

12.3 Strumenti Citati

- Bitwarden: bitwarden.com | 1Password: 1password.com | KeePassXC: keepassxc.org
- Aegis Authenticator: getaegis.app | YubiKey: yubico.com
- ProtonMail / ProtonDrive: proton.me | Tresorit: tresorit.com
- ProtonVPN: protonvpn.com | Mullvad: mullvad.net
- Nextcloud: nextcloud.com | Signal: signal.org
- Ollama (AI locale): ollama.ai

12.4 Log delle Revisioni

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

Centuria Foundation

centuriafoundation.pl