# Posizione AIPSI
## sulla bozza AgID
## "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"

Milano, 12/11/2019

# Indice

## Sommario

# Introduzione

Il presente documento fornisce commenti e suggerimenti di modifiche al documento in consultazione (bozza) AgID su "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" preparati da un Gruppo di Lavoro (GdL) AIPSI costituito da:

- Ing. Marco R.A. Bozzetti, Presidente Aipsi
- Massimo Chirivì, Consigliere Aipsi
- Dott. Francesco Zambon, Socio Aipsi

Nell'Allegato 1 del presente documento una breve descrizione di AIPSI, e nell'Allegato 2 una scheda sintetica dei componenti del GdL per evidenziare le loro competenze ed esperienze sul tema.

Il GdL ha fatto riferimento al documento in bozza in https://docs.italia.it/AgID/documenti-in-consultazione/lg-documenti-informatici-docs/it/bozza/
ed ai suoi Allegati in https://docs.italia.it/AgID/documenti-in-consultazione/lg-documenti-informatici-docs/it/bozza/allegati.html

I commenti ed i suggerimenti nel seguito descritti, ed evidenziati in corsivo, non hanno la pretesa di essere completi ed esaustivi, e vogliono fornire un contributo della nostra associazione di professionisti della sicurezza digitale al miglioramento di questo importante documento.

# Considerazioni Generali

Le linee guida dovrebbero essere un documento operativo ed auto-esplicativo, chiaro e senza difficoltà di interpretazione, su che cosa bisogna fare e come, utilizzabile non solo da personale tecnico, ma ad esempio anche da personale dell'organizzazione, dai responsabili/referenti delle varie direzioni, dai referenti della privacy e dall'eventuale DPO, Data Protection Officer, (responsabile della protezione dei dati) per la privacy.
Nel seguito sono riportate le principali considerazioni generali evidenziate dal GdL, che in estrema sintesi suggerisce che il **presente documento sia sostanzialmente rivisto e semplificato** perché possa costituire realmente una efficace e seguibile linea guida.

1. La presente bozza non considera e non esplicita chiaramente l'intero "ciclo di vita" di un documento informatico, e soprattutto non fa riferimento ad alcuna procedura organizzativa per la sua definitiva eliminazione dai sistemi che lo archiviano. Nel titolo lo stesso termine "formazione" risulta in parte ambiguo, e si suggerisce di sostituirlo con "*creazione*"
    a. Si suggerisce quindi di cambiare l'intero titolo delle linee guida in ***Linee guida sulla creazione, gestione, conservazione ed eliminazione dei documenti informatici***
2. La presente bozza fa ampi e dettagliati riferimenti alla legislazione precedente (ma non sempre in maniera aggiornata, si veda nel seguito), ma inutili e fuorvianti a livello operativo. Si suggerisce pertanto di porre tutti questi riferimenti normativi in un allegato ad hoc, ma nelle linee guida di riportare solo i contenuti che devono essere seguiti.
3. Nella bozza sulle linee guida sono evidenziati molti principi generali, condivisibili, ma poche scelte ed indicazioni precise, di che cosa e come si deve fare in pratica!.
4. Al di là dei riferimenti alle varie normative, l'attuale bozza, inclusi gli allegati, rappresenta più una ampia raccolta di che cosa è presente sul mercato (si veda ad esempio l'elenco dei vari formati di file), più che una guida tecnica e precisa che dettagli le poche scelte rilevanti che devono essere attuate. Questo richiede che AgID, in accordo con gli altri ministeri, ed oggi in particolare con quello della dell'Innovazione tecnologica e digitalizzazione, definisca i soli, pochi, formati e standard da utilizzare nella stragrande parte delle PA e del più comune utilizzo di documenti, che sono tipicamente testi con immagini, e con eventuali link a parti con filmati, voci, etc. Tenendo anche conto che, giustamente, la PA dovrebbe utilizzare solo prodotti opensource, ed invece fa larghissimo uso di prodotti proprietari, in primis di Microsoft.
    a. L'approccio seguito è di considerare tutti i possibili documenti multimediali, filmati inclusi. Si suggerisce di individuare il sottoinsieme più diffuso (ad esempio docx e pdf)

, considerando tutti gli altri come casi speciali da considerare se e solo se strettamente necessario.

5. Nella bozza sono pochi i riferimenti ai determinanti aspetti della sicurezza digitali dei documenti informatici. Il documento non esplicita chiaramente come rendere sicuro un singolo documento o un gruppo di documenti, ad esempio attraverso la loro criptazione o firmandoli con certificati, classificando il livello di riservatezza richiesto/necessario, anche, ma non solo, in logica GDPR per dati personali e sensibili. Si suggerisce di creare un capitolo ad hoc dal titolo "La sicurezza digitale del documento informatico" (o titolo simile), nel quale dettagliare le modalità prescelte per classificare i documenti nell'ottica della loro riservatezza, e come criptarli coi certificati (anche con riferimento a SPID livello 3).
6. Si suggerisce di distinguere le misure di sicurezza tecnica relative ai software che creano e trattano i documenti dalle misure relative alle infrastrutture ICT che li supportano, dalle reti ai server.
7. Per il contenuto degli allegati tecnici, non sono previste regole e metodi per aggiornarli. Si suggerisce una revisione bi/triennale, che dovrebbe evidenziare le scelte obsolete o in via di obsolescenza e quelle valide oggi (alla data) e nel prossimo futuro.

# Specifici suggerimenti/correzioni proposte

Al di là delle considerazioni generali di cui sopra, che suggerisco una reimpostazione del documento, nel seguito vengono dettagliati specifici cambiamenti. Il testo di riferimento del documento riportato è evidenziato in giallo, il cambio proposto è in corsivo.
L'elenco non è sicuramente esaustivo, e sono stati considerati i temi ritenuti dal GdL più significativi.

1. Riferimenti alla normativa esistente. Come già indicato nelle considerazioni generali, l'intero Capitolo 1, o un allegato ad hoc, dovrebbe accorpare tutti i riferimenti legislativi, che non dovrebbero poi essere menzionati nelle linee guida che seguono. Sui vari riferimenti comunque si è rilevato quanto segue.

- **Capitolo 1.4**: Abrogazioni e norme transitorie. Il seguente paragrafo potrebbe creare delle incomprensioni:
  - A partire dalla data di applicazione delle presenti Linee Guida, sono abrogati:
  - il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici21";
  - il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione", ad eccezione dell'art. 13 che rimane in vigore fino alla emanazione delle Linee guida di cui all'art. 29 del CAD. (qui si comprende che il DPCM si abroga tutto escluso l'art. 13)
    Per quanto concerne il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", a partire dalla data di applicazione delle presenti Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:
    - art. 2 comma 1;
    - art. 6;
    - art. 9;
    - art. 18 commi 1 e 5;
    - art. 19;
    - art. 20;
    - art. 21.

      (qui, oltre all'articolo 13 vengono aggiunte altre esclusioni).

  Si suggerisce di modificarlo in:
  - *A partire dalla data di applicazione delle presenti Linee Guida, sono abrogati:*
  - *il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici21";*
  - *il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione", ad eccezione dell'art. 13 che rimane in vigore fino alla emanazione delle Linee guida di cui all'art. 29 del CAD e dei seguenti articoli: art. 2 comma 1, art. 6, art. 9, art. 18 commi 1 e 5, art. 19, art. 20 e art. 21.*

2. **Mancano i riferimenti alle seguenti normative**:
   a) modifiche effettuate al Codice dell'Amministrazione Digitale (D.lgs 82/2005) e precisamente il D.lgs n. 217 del 13 dicembre 2017 e il D.lgs 179 del 26 agosto 2016;
   b) Decreto legislativo 10 agosto 2018, n. 101;
   c) Decreto legislativo n. 97 del 2016 - FOIA (Freedom of Information Act)
   d) NIS e European Cybersecurity Act, anche se non dettagliano specifiche misure tecniche

3. **Cap. 2: identificazione di un documento**
   a) **Paragrafo 2.1.1**:
      - Titolo: si suggerisce di sostituire Formazione con *Creazione*
      - testo attuale:

        ……. Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente accoppiata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione documentale. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di hash che siano ritenute crittograficamente sicure. Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione. ……

        Si suggerisce di meglio chiarirlo con il seguente testo:

        *Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente accoppiata al documento. Per il documento creato e protocollato deve essere generata l'impronta che deve essere salvata insieme alla segnatura, in modo da garantire la immodificabilità del documento anche da soggetti con permessi elevati. Dopo aver generato la segnatura e attivata la funzione di generazione dell'impronta dotata di salatura implementata dal sistema gestionale, il sistema non deve permettere la modifica di tale documento.*

   **b)** Medesimi problemi si riscontrano **nelle modalità b), c), e d) del paragrafo 2.1.1**, che impattano anche sulla copia digitale di documenti cartacei, ripresi nei Cap. 2.2 e 2.3, e nel relativo processo in Allegato 3 (si veda punto 4 successivo)
   c) Considerazioni sulla **difficoltà/impossibilità di identificare in maniera univoca e persistente un documento informatico senza specifici strumenti di gestione documentale.** In molti casi, ed in particolare nelle piccole strutture della PA, la maggior parte dei documenti sono creati tramite strumenti di informatica individuale quali, ad esempio, Microsoft Word, Excel, Power Point, Libre ed Adobe, e sovente copiando ed adattando i contenuti da siti web … e ci si ferma a questi sistemi, a parte l'eventuale successiva firma digitale del documento. Risulta quindi

difficile/impossibile poter assicurare il basilare e sacrosanto principio di univoca e persistente identificazione del documento, a meno che non venga inserito nel protocollo informatico. E' opportuno quindi che si diano istruzione chiare e precise. Due, ad esempio, le possibili ipotesi, non esclusive tra loro:

- Che *ogni documento informatico "finale" e "ufficiale" (quindi non bozze) sia obbligatoriamente inserito nel protocollo informatico*;
- Che sia *obbligatorio l'uso di sistemi documentali, per esempio Alfresco in open source, per la gestione di tutti documenti informatici dell'organizzazione.*

4. **Cap. 2.2, Cap. 2.3 e Allegato 3**. Come anticipato in b) del punto precedente, non sono chiari alcuni aspetti delle procedure pratiche da seguire, anche in termini di responsabilità. quale procedura applicare nel caso in cui debba essere prodotta una copia digitale di una vecchia delibera di cui ci si presta ad effettuare una scansione con una multifunzione: l'utente addetto dovrebbe generare l'impronta del documento generato dalla scansione e firmare i 2 file con firma digitale propria in modo da registrare l'operatore che sta facendo la trasformazione del documento da cartaceo a digitale. Un'ulteriore considerazione: nel caso di una seconda scansione dello stesso documento, verrebbe generata una seconda impronta, diversa dalla prima. Ci potrebbero essere problemi in caso di contenzioso? In questo caso il concetto di ripetibilità verrebbe meno.

5. **Cap. 2.4 e 2.5.** Documenti amministrativi. In riferimento ai documenti con attinenza a standard precisi, ad esempio fatture elettroniche, XML AVCP o altro, sarebbe opportuno innalzare i livelli di sicurezza in quanto, ormai, un malware potrebbe essere in grado di alterare con assoluta semplicità il contenuto degli stessi, ad esempio modificando le coordinate bancarie presenti in un file XML di una fattura elettronica. È prassi in molte amministrazioni pubbliche salvare i file XML in apposite share di rete che potrebbero essere raggiunte da un malware. Quest'ultimo potrebbe modificare con tutta semplicità il contenuto dei files in quanto la stessa struttura dell'XML risulta essere standardizzata e conosciuta perché oggetto di progetti di pubblico dominio. Si suggerisce pertanto di precisare le misure di sicurezza da usare concretamente per proteggere questi documenti.

6. **Paragrafo 3.1.6** : Requisiti minimi di sicurezza dei sistemi di protocollo informatico. Fa riferimento al Cap. 3.9 della bozza, che a sua volta fa riferimento "Misure minime di Sicurezza ICT per le pubbliche amministrazioni", circolare 18 aprile 2017, n° 2/2017 dell'Agenzia per l'Italia Digitale, commentata da AIPSI al successivo punto 6 di questa nota. Si sottolinea come lo stesso par. 3.1.6 evidenzia come il protocollo informatico debba garantire "la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;". Ma quali strumenti di controllo degli accessi, in termini di identificazione, autenticazione e autorizzazione" devono in pratica essere considerati? Queste linee guida dovrebbero indicarlo chiaramente. Si veda anche il suggerimento del punto 6 nelle considerazioni generali.

7. **Cap. 3.2**: Classificazione dei documenti informatici. Nell'ambito della classificazione del documento **è essenziale stabilire il livello di riservatezza del documento** considerato (o del

gruppo di documenti), sia per l'analisi dei rischi sia per le misure di sicurezza che devono essere applicate. Nel capitolo non se ne parla. Occorre aggiungere un paragrafo ad hoc fissando i livelli di riservatezza. A livello nazionale sono distinti in termini di segretezza i documenti classificati da quelli non classificati, che quindi possono essere "pubblici. Per quelli classificati la norma prevede:

- segretissimo (SS)
- segreto (S)
- riservatissimo (RR)
- riservato (R)

Si veda: https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni/classifiche-di-segretezza.html

8. **Cap. 3.3.4**: Archivio informatico. Non si cita la **fondamentale necessità di back-up periodici**, e delle relative procedure di ripristino, soprattutto per gli archivi informatici "correnti". La realtà è che nella maggior parte dei casi delle PA piccole i back-up sono effettuati in maniera incompleta, sovente senza disporre di un hard disk removibile e depositato in un luogo diverso da quello ove si trovano i sistemi informatici. Molti pensano poi che la replica su sistemi terziarizzati/in cloud renda inutile il back up: grave errore, dato che, se questi sistemi terzi sono sempre collegati a quelli del cliente, malware li possono direttamente attaccare. I molti casi di ransomware andati a buon fine per gli attaccanti ne sono un esempio. Si suggerisce di redigere un paragrafo ad hoc sul tema, da inserire o in 3.9 o in un capitolo ad hoc di 1° livello nell'indice.

9. **Cap 3.9:** Misure di sicurezza.
   a) Sono state prese come riferimento le "Misure minime di Sicurezza ICT per le pubbliche amministrazioni", circolare 18 aprile 2017, n° 2/2017 dell'Agenzia per l'Italia Digitale (Punto 18 dei riferimenti normativi). Bisogna considerare però che tale circolare fu redatta con un riferimento preciso alla SANS 20 - CIS Critical Security Controls for Effective Cyber Defense - versione 6.0 di ottobre 2015 ormai obsoleta in quanto è stata pubblicata la versione 7.1 di Aprile 2019 che innanzitutto modifica la struttura ed identificazione dei controlli nei punti #3,#4,#5, e soprattutto identifica le organizzazioni in 3 gruppi:
      - A family-owned business with ~10 employees may self-classify as IG1;
      - A regional organization providing a service may classify itself as IG2;
      - A large corporation with thousands of employees may be labeled IG3.

      Con livelli di controllo naturalmente diversi per i diversi gruppi. Tenendo conto che gran parte della PA rientrerebbe nel gruppo IG2, bisogna considerare che i controlli di cui alla versione 7.1 di Aprile 2019 (https://www.cisecurity.org/controls/) focalizzano l'attenzione su una maggiore consapevolezza dei rischi legati alle procedure di autenticazione ed accessi privilegiati. Si veda nuovamente il suggerimento del punto 6 nelle considerazioni generali.
   b) Dettagliare il cap. 3.9 della bozza in maniera più approfondita riprendendo ABSC 10 (CSC 10): COPIE DI SICUREZZA dalle "Misure minime di Sicurezza ICT per le pubbliche

amministrazioni", circolare 18 aprile 2017, n° 2/2017 dell'Agenzia per l'Italia Digitale, e creando un enforcement delle stesse con le modifiche emanate con la versione 7.1 di Aprile 2019 degli stessi controlli, i quali innalzano il livello di sicurezza su tutti i punti del controllo

c) Dettagliare ulteriormente questo cap. con i temi del backup e del ripristino da backup, e del controllo degli accessi, oppure creare un capitolo ad hoc di primo livello nell'indice

10. **Allegato 2**: Formato dei files. Come già evidenziato, presenta una rimarcabile lista di un gran numero dei formati dei files, ma manca una sintesi chiara delle indicazioni che devono essere seguite.
    a) Sarebbe inoltre utile ed opportuno aggiungere una guida tecnica su come convertire formati obsoleti, proprietari o sconsigliati ai formati consigliati.

11. **Allegato 4**: Standard e Specifiche tecniche. Gli standard evidenziati, soprattutto in 3.1, non considerano gli aspetti di identificazione, autenticazione ed autorizzazione per il controllo degli accessi ai sistemi informatici che trattano i documenti informatici, ed il cui superamento è una delle principali cause di attacchi informatici intenzionali in Italia (si vedano gli ultimi Rapporti annuali OAD in https://www.oadweb.it/it/). Si suggerisce di indicare nel paragrafo 3.1 dell'Allegato 4 almeno i consolidati (da anni) standard SPML, SAML, XACML, oltre ai simili WS-Fed e WS-Trust: sono basilari per l'autenticazione federata, il Single Sign On sicuro e per l'interoperabilità standard tra codici diversi operanti su sistemi operativi diversi via web services. Da valutare se considerare i relativamente "nuovi" standard per il controllo degli accessi quali ad esempio NGAC, Next Generation Access Control, a sua volta basato su XACML.

# Allegato 1 AIPSI

**AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (**https://www.aipsi.org/**),** è **u**na Associazione apolitica, aconfessionale e senza fini di lucro cui possono associarsi solo persone fisiche, non giuridiche, che a vario titolo si occupano di sicurezza digitale.

AIPSI è **Capitolo Italiano** di **ISSA**, Information Systems Security Association, (www.issa.org) che conta circa 13.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo

**Obiettivo principale** di AIPSI è aiutare i propri Soci nella loro **crescita professionale,** fornendo concreti **strumenti** per l'aggiornamento delle competenze e per creare una comunità con relazioni interpersonali tra professionisti, anche a livello internazionale, tale da favorire ed aiutare la carriera e la crescita di opportunità di business per il Socio.

In tale ottica, AIPSI offre ai propri Soci un insieme di **servizi qualificati,** anche grazie a quanto fornisce ISSA, che includono:

- Convegni, workshop, webinar sia a livello nazionale che internazionale (via ISSA)
- **ISSA Journal**, l'autorevole e prestigiosa rivista mensile dell'Associazione riservata ai Soci
- La newsletter mensile
- Il servizio **AIPSIAlert** via Telegram per tempestivamente informare sulle più recenti vulnerabilità e criticità ICT riscontrate e come porvi rimedio
- Indagini con relativi rapporti annuali, fra le quali:
  - L'indagine annuale **OAD, Osservatorio Attacchi Digitali in Italia**, giunta all'undicesimo anno consecutivo, effettuata in collaborazione con la Polizia Postale e delle Telecomunicazioni, Malabo Srl, Reportec Srl e con il patrocinio di numerose associazioni. OAD dispone di un suo specifico sito web, https://www.oadweb.it, che costituisce l'archivio di tutti i Rapporti annuali e delle numerose presentazioni effettuate in eventi nazionali ed internazionali, ed articoli pubblicati in merito
  - **ESG ISSA Survey** "The Life and Times of Cyber Security Professionals"
  - Indagine in corso sulla **professione femminile nella cybersecurity in Italia (CSWI)**
- Concreto supporto nell'intero ciclo di vita professionale, con formazione specializzata e **supporto alle certificazioni**, in **particolare eCF Plus (EN 16234-1:2016)** con AICA
- Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte.

# Allegato 2

Sintetici curricula dei componenti del Gruppo di Lavoro AIPSI
che hanno stilato la presente nota

# Marco Rodolfo Alessandro Bozzetti

Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico laureato al Politecnico di Milano, è fondatore e amministratore di Malabo S.r.l (www.malaboadvisoring.it), società di consulenza direzionale sull'ICT (Information and Communication Technology) creata a marzo 2001. Attraverso Malabo, Marco ha condotto e conduce interventi consulenziali presso Aziende ed Enti lato sia offerta sia domanda ICT. Marco ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e GEA/GEALAB, oltre ad essere stato il primo responsabile dei sistemi informativi dell'intero Gruppo ENI (1995-2000). In tale posizione ha realizzato la terziarizzazione delle infrastrutture ICT dell'intero Gruppo (più di 22 Data Center) e della rete di comunicazione italiana in fibra ottica: a quella data una delle più grandi terziarizzazioni in Italia e in Europa. Agli inizi della sua carriera, in ambito Olivetti e del CREI del Politecnico di Milano, è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, a partire dalla sua tesi di laurea. Nel corso della sua carriera Marco ha fondato e ha diretto o è stato partner di alcune aziende dell'offerta ICT, tra le quali CA.SI, Ibimaint System Engineering, ClickICT. A livello consulenziale innumerevoli gli interventi tecnici-organizzativi sui sistemi informatici di medie e grandi Aziende private, oltre che di alcuni Enti pubblici. aventi il principale obiettivo di allineare l'ICT al business, di innovarlo e di generare valore effettivamente misurabile. I principali campi di intervento includono il governo e la gestione del sistema informatico, la sicurezza digitale, l'analisi e gestione dei rischi ICT e dei loro impatti (BIA), il disegno di architetture ICT, la razionalizzazione del sistema informatico, la definizione ed il supporto di strategie ICT, l'assessment delle tecnologie, delle competenze e dei ruoli ICT, l'analisi del valore per l'ICT, l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi, il supporto per la compliance alle varie normative, in particolare alla privacy (secondo il GDPR, General Data Protection Regulation). Negli anni '90 e fino al 2003 ha ideato e coordinato per SMAU EITO, European Information Technology Observatory, l'indagine annuale sul mercato ICT e sui suoi trend; Marco è stato il curatore scientifico dell'intera opera. Dal 2009 in collaborazione con Malabo, AIPSI, Polizia Postale ed altri Enti ed associazioni, ha ideato e realizzato OAD, Osservatorio Attacchi Digitali in Italia: è un'indagine via web, totalmente anonima e rivolta a tutti i settori merceologici, Pubbliche Amministrazioni incluse, che produce annualmente un rapporto indipendente sul fenomeno degli attacchi digitali intenzionali in Italia. Da gennaio 2016 Marco con Malabo guida un progetto per il CNF, Consiglio Nazionale Forense, attraverso la sua Fondazione per l'innovazione FiiF. Il compito è di riprogettare il sistema informatico interno e di realizzare innovativi servizi digitali per gli Ordini e gli Avvocati, nell'ottica di fornire una concreta spinta innovativa nella trasformazione digitale dell'avvocatura italiana. Marco è stato Presidente e VicePresidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.

È attualmente Presidente di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica e Capitolo Italiana della mondiale ISSA, e nel Consiglio Direttivo di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio e revisore dei conti del ClubTI di Milano, socio AICA.

È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser". E' Commissario d'Esame in AICA per le certificazioni eCFPlus (EN 16234-UNI 11506).

Ha pubblicato più di 200 articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT.

*Ai fini della legge sulla privacy, si autorizza l'uso e la circolazione del presente curriculum vitae*

# Massimo Chirivì

Massimo Chirivì è Consigliere AIPSI e CEO Innovamind srls, Società Partner di Malabo Srl. Nel 1996 Chirivì inizia l'attività di Consulente Informatico ed intraprende un percorso formativo personale che lo porta oggi ad essere un sistemista, esperto di sicurezza, privacy e sistemi ICT. Dal 1996 al 2006 è stato amministratore unico della Dipartimento Informatica sas, società operante nel settore dei servizi per l'informatica. Dal 1998 si occupa di Innovazione Tecnologica nella P.A. ed è referente ICT per diversi progetti comunitari. Dal 1999 al 2012 è stato esaminatore accreditato AICA e nel 2009 è stato nominato esaminatore qualificato. Dal 1999 si occupa di sviluppo, aggiornamento e indicizzazione di siti e portali web. Dal 2002 è impegnato nel progetto Misatel, una Web Application (CRM-ERP). Dal 1996 ad oggi sono centinaia seminari, workshop, corsi, forum, e webinar a cui ha partecipato per arricchire le proprie conoscenze Dal 2004 al 2007 ha collaborato con Prometeo SPA (TV) come partner tecnico/commerciale per la Puglia. Dal 2006 è consulente e libero professionista nel settore informatico. Oltre alle attività di consulenza è dal 2001 docente ed esperto esterno in vari progetti formativi sia di Istituti Scolastici Statali che di Enti di Formazione Professionale. Dal 2008 è entrato a far parte di diverse Associazioni nazionali ed internazionali tra cui l'ICAA, il CLUSIT, l'AICA, Federprivacy, ISSA, e AIPSI. Dal 2002 svolge il ruolo di CTP in controversie legali. Dal 2007 è consulente e responsabile dei sistemi informativi della BRB HOLDING. Dal 2009 è System Integrator su sistemi DELL, azienda con cui si è formato in Polonia nel 2009. Dal 2010 al 2015 è stato consulente nel Gruppo I&T con sedi in Italia e Francia dove ha occupato il ruolo di: System Administrator su S.O. Microsoft e Linux; Web Server Administrator su tecnologie IIS, Tomcat, Apache; DBMS Administrator Microsoft Sql Server, MySql, PostgreSQL; Sviluppatore di portali CMS e con una particolare attenzione ai problemi di accessibilità nei siti web della P.A.
Dal 2015 è Founder & CEO della Startup Innovamind srls, azienda che si occupa di Sicurezza Informatica, Ricerca e Sviluppo. Dal 2011 ad oggi è stato relatore in 13 tappe SMAU in diverse città d'Italia, in 2 Privacy Day Forum organizzati da Federprivacy tra cui l'edizione 2019 al CNR di Pisa, e numerosi altri convegni e seminari.
Dal 15 gennaio 2016 è membro del Consiglio Direttivo Nazionale di AIPSI (Associazione Italiana Professionisti Sicurezza Informatica).
Dal 2018 è DPO e consulente GDPR per alcune aziende e pubbliche amministrazioni
Esperto tecnico ISO 27001-27017-27018, collabora in attività di Audit in Italia e Albania.
Dal 2018 collabora con Musa Formazione come docente per corsi Ethical Hacking & Security Manager.
La lunga esperienza sul campo ha contribuito a formare ed arricchire le conoscenze personali, le capacità nelle relazioni interpersonali e nelle dinamiche di gruppo, l'ottimizzazione della didattica, le ricerche di metodologie didattiche innovative e le svariate tecnologie informatiche su cui si è potuto confrontare con colleghi e problemi aziendali di ogni genere. Le innumerevoli novità del mondo ICT e le continue sfide del progresso informatico lo hanno indotto ad un aggiornamento quotidiano sulle nuove tecnologie.
Passione, condivisione, professionalità ed etica sono i principi essenziali attorno cui ruota, costantemente, il suo modus operandi.

*Ai fini della legge sulla privacy, si autorizza l'uso e la circolazione del presente curriculum vitae.*

# Francesco Zambon

Francesco Zambon, laureato in matematica alla Facoltà di Scienze dell'Università di Padova, svolge attività di consulenza nell'ICT in Italia e all'estero anche come Partner di Malabo Srl, in particolare per la governance dei processi di erogazione dei servizi ICT e per il supporto della sicurezza digitale logica, fisica ed organizzativa.

Ha concluso la sua carriera da dirigente in ENI Spa, dove ha collaborato all'unificazione di tutte le risorse informatiche a livello mondiale come responsabile dell'adozione di tecnologie innovative utilizzate su larga scala. Ha inoltro fornito supporto tecnologico alla sicurezza ICT di ENI per quanto riguarda sia l'identificazione e l'implementazione delle soluzioni tecniche che per quanto riguarda le normative architetturali e di utilizzo. Precedentemente ha operato, con responsabilità crescenti, in Enidata e in Tema Spa.

E' stato per due anni consulente della Comunità Europea nei settori dell'intelligenza artificiale e del calcolo parallelo ed per l' ESA, Ente Spaziale Europeo, a Parigi e a Darmstadt, si è occupato per il progetto Meteosat del sistema di controllo del satellite, della sua progettazione e realizzazione, ed è stato responsabile dei rilasci conclusivi.

Ha svolto attività didattica per diverse università a Milano, Roma, Bologna e Modena.

Ha pubblicato articoli sull'informatica e sulla sua sicurezza, ed è attualmente socio di ACM, AIPSI, IEEE, CS, Computer Society, e del ClubTI di Milano.

*Ai fini della legge sulla privacy, si autorizza l'uso e la circolazione del presente curriculum vitae.*