CYBERSECURITY E INTELLIGENZA ARTIFICIALE

Le sfide e le opportunità per il settore finanziario ed assicurativo tra innovazione tecnologica e normative europee

23 ottobre 2024

Seminario in videoconferenza

La normativa cybersecurity nel settore bancario e assicurativo affronta una fase di profonda innovazione legata all'adozione di norme che responsabilizzano fortemente chi gestisce sistemi informatici, chiamandolo a prevenire i rischi connessi all'uso di questi strumenti. In particolare, GDPR, IA ACT, NIS2 e DORA sono norme che per il settore bancario e assicurativo comportano la necessità di affrontare con consapevolezza le sfide attuali e future legate alla cybersecurity in due dei settori più sensibili alla gestione dei dati e della sicurezza operativa.

Argomenti

L'incontro intende affrontare questi argomenti essenziali:

1. **Regolamenti e normative europee e nazionali**: Focus su **GDPR**, **IA ACT, NIS2** (Network and Information Security Directive) e altre normative specifiche per il settore finanziario come il **Regolamento DORA** (Digital Operational Resilience Act). Analisi delle implicazioni pratiche per banche e assicurazioni.

2. **Gestione del rischio cyber e del rischio connesso ai sistemi di intelligenza artificiale**: Come le istituzioni finanziarie possono identificare, valutare e mitigare i rischi legati agli attacchi informatici e all'uso di sistemi di intelligenza artificiale. Integrazione delle linee guida **EBA** (European Banking Authority) e **EIOPA** (European Insurance and Occupational Pensions Authority).

3. **Incident Response e gestione delle crisi**: Procedure per la gestione degli incidenti di sicurezza informatica, la comunicazione con le autorità competenti e la ripresa operativa post-attacco. Case study di incidenti reali.

4. **Cybersecurity e innovazione tecnologica**: Impatto delle tecnologie emergenti come **blockchain**, **intelligenza artificiale** e **cloud computing** sulla sicurezza e conformità normativa nel settore finanziario.

5. **Partnership pubblico-private e condivisione di informazioni**: Collaborazione tra aziende, governi e istituzioni per migliorare la resilienza informatica attraverso lo scambio di dati e informazioni sugli attacchi e le vulnerabilità.

6. **Formazione e sensibilizzazione del personale**: Strategie per creare una cultura della sicurezza all'interno delle organizzazioni, con particolare attenzione alla formazione dei dipendenti sul riconoscimento e la gestione dei rischi informatici.

7. **Cybersecurity e privacy dei dati dei clienti**: Equilibrio tra la protezione dei dati personali dei clienti e la conformità alle normative, garantendo al contempo un'efficace protezione contro le minacce informatiche.

8. **Impatto delle violazioni normative e delle sanzioni**: Analisi dei casi in cui banche e assicurazioni non hanno rispettato le normative sulla cybersecurity, con focus sulle conseguenze economiche e reputazionali.

9. **Cyber-insurance**: L'emergente mercato delle assicurazioni contro i rischi cyber, i modelli di pricing e copertura, e le sfide nel valutare i rischi informatici per il settore assicurativo.

10. **Standard di sicurezza e certificazioni**: Approfondimenti sui principali standard internazionali, come **ISO/IEC 27001** e **PCI DSS**, e sul loro impatto nel settore bancario e assicurativo.

Obiettivo
Fornire a professionisti del settore finanziario un quadro aggiornato delle normative sulla cybersecurity, l'intelligenza artificiale, le best practice per la gestione dei rischi connessi all'utilizzo di tecnologie e agli incidenti informatici, e approfondimenti sulle sfide future legate all'innovazione tecnologica

Interventi

9:30 - 9:45 | Apertura e Benvenuto

- Breve introduzione agli obiettivi del convegno e al contesto normativo attuale.

9:45 - 10:15 | Sessione 1: Quadro Normativo Europeo e Nazionale per la Cybersecurity e l'Intelligenza Artificiale

- Panoramica delle normative principali: GDPR, IA ACT, NIS2, DORA, e loro impatto sulle istituzioni finanziarie.
- Discussione sulle sfide operative per la conformità.

10:15 - 10:45 | Sessione 2: Approfondimento sull'IA ACT.

- Il Regolamento UE 2024/1689. Il regolamento europeo sull'Intelligenza Artificiale.
- Descrizione del Regolamento e del suo ambito di applicazione.
- Obiettivi principali e impatti previsti.
- Requisiti principali per le istituzioni bancarie e assicurative.
- Normative specifiche sulla protezione dei dati e sulla gestione degli incidenti.
- Conformità e obblighi di reporting.

10:45 - 11:00 | Pausa Caffè

11:00 - 11:45 | Sessione 3: Cyber Risk Management e IA Governance nel Settore Bancario e Assicurativo

- Come identificare e valutare i rischi cyber specifici per il settore finanziario.
- Linee guida delle autorità di vigilanza (EBA ed EIOPA) per la gestione dei rischi informatici.
- Il report di EIOPA sulla Governance dell'Intelligenza Artificiale. EIOPA.
- Il report EBA sul machine learning.

11:45 - 12:30 | Sessione 4: Innovazione Tecnologica e Cybersecurity: Cloud, Blockchain, e AI

- Impatti delle nuove tecnologie sulla sicurezza e sulla conformità alle normative.
- Come le banche e le assicurazioni possono sfruttare l'innovazione senza compromettere la sicurezza.
- Come garantire la compliance normativa nella gestione degli incidenti e nella valutazione dei rischi cyber e nella governance dell'intelligenza artificiale.

12:30 | Chiusura e Networking

Relatori

MARCO MAGLIO
Avvocato in Milano e fondatore di Lucerna Iuris, il primo Network Giuridico Internazionale formato da legali di tutti i Paesi dell'Unione Europea specializzati in assistenza legale per le attività compliance, comunicazione commerciale e per il trattamento dei dati personali. E' professore a contratto di Diritto della protezione dei dati personali e tiene corsi di specializzazione in Italia e all'estero come docente nelle materie di Data Protection e Privacy Engineering, Diritto dei consumi e del marketing e Diritto della sicurezza alimentare. E' presidente dell'Osservatorio Europeo sulla Data Protection.

LUCA SEVERINI
Specialista di sicurezza informatica. Ha seguito numerosi progetti condotti in diverse amministrazioni pubbliche e imprese finalizzati all'introduzione di metodi, tecnologie e sistemi per garantire i livelli di sicurezza delle infrastrutture, delle comunicazioni e per la protezione dei dati personali. HA maturato esperienza nella a gestione di progetti di ricerca nel campo delle ICT, finalizzati alla realizzazione di sistemi per il trattamento di dati arricchiti semanticamente (linked data) e di sistemi basati su conoscenza (ontology-based system), collaborando con il Centro di Ricerca di Cyber Intelligence and Information Security (CIS)

PATRIZIA GHINI
Titolare dello Studio Patrizia Ghini (studio di consulenza direzionale e organizzazione aziendale), nel quale svolge l'attività di consulenza aziendale e societaria, Commercialista, Revisore dei conti e Giornalista pubblicista, specializzata in una serie di temi riferibili alla cd. "etica d'impresa" (privacy; responsabilità amministrativa degli enti; corporate & control governance; compliance; whistleblowing;).
E' membro di Collegi sindacali ed Organismi di Vigilanza ai sensi del D.Lgs. 231/2001 e Responsabile della Protezione dei dati personali.

(Questo convegno è finanziabile attraverso i vouchers del Fondo Banche e Assicurazioni)

Quota di partecipazione Euro 400,00 + IVA 22% a partecipante
Sono previste scontistiche per piu' partecipanti della medesima azienda

E' possibile procedere all'acquisto degli atti dei convegni inviando la richiesta a segreteriagenerale@iside.it
I webinar saranno fruibili sulla piattaforma Zoom
Ulteriori informazioni al numero 02.80016480 e segreteriagenerale@iside.it o www.iside.info

ISIDE srl
Via Dante n.4 - 20121 Milano
Tel 02.80016480 - Fax 02.80016481

Azienda certificata ISO 9001
Certificato n° IT20-24804A