Infosec & Quality [ITA] - Mag. 2023

16 MAY 2023

Juvenilia. Prima della partita. Maggio 2023. Foto non mia

Indice

In aprile si sono conclusi i meeting semestrali del WG 1 e del WG 5 del ISO/IEC JTC 1 SC 27. Si tratta dei gruppi che seguono le norme ISO/IEC 27001, 27002, 27005 eccetera e le norme sulla privacy, inclusa la ISO/IEC 27701.

Per quanto riguarda il WG 1, le attività si sono svolte online e, in realtà, il meeting è servito a sintetizzare le attività svolte in altri incontri da ottobre.

Si sono avviati i lavori per la revisione di ISO/IEC 27000 (panoramica sui SGSI), 27003 (guida alla 27001) e 27004 (sulle misurazioni). Si tratta di norme molto importanti.

Si è poi deciso di non avviare i lavori per una nuova ISO/IEC 27001, anche se la versione del 2022 era stata approntata rapidamente per aggiornare l'Annex A seguendo alla nuova ISO/IEC 27002 e recepire le modifiche all'HLS.

Ci è stato comunicato che, a livello IAF (ossia l'ente che promuove e controlla le attività di accreditamento), sono stati uniti i gruppi che si occupano di ISO/IEC 27001 e ISO/IEC 20000 per ottenere una maggiore coerenza negli accreditamenti relativi alla sicurezza dei dati e all'informatica. Viene da ridere, pensando che molti vorrebbero che la ISO/IEC 20000-1 si occupi di servizi in generale e che la ISO/IEC 27001 non si occupa solo di sicurezza informatica (o cybersecurity).

Per quanto riguarda le attività del WG 5, che si occupa di privacy, sono proseguiti i lavori per la ISO/IEC 27006-2 (ossia le regole di accreditamento). Sono stati avviati i lavori per una norma sulla privacy e intelligenza artificiale (ISO/IEC 27091). Ho notato poi molto lavoro per gli standard relativi alla verifica dell'età.

Importante, a mio avviso, è il lavoro in fase di conclusione per la ISO/IEC 27701, ossia la norma per la certificazione dei sistemi di gestione per la privacy (estensione della ISO/IEC 27001). Infatti la norma passa in stato di FDIS e quindi entro fine anno dovrebbe uscirne la versione aggiornata. Non bisogna aspettarsi nulla di nuovo se non l'allineamento alle ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Su questo fronte, i lavori per l'aggiornamento della ISO/IEC 27018 (privacy per fornitori di servizi cloud, estensione della ISO/IEC 27002) procedono a rilento.

Sarà pubblicata una nuova versione della ISO/IEC 29134 sulla DPIA, ma riporterà solo aggiornamenti non significativi rispetto all'edizione attuale (su questo avevo già scritto in passato che è un peccato, visto che la norma richiederebbe un aggiornamento significativo, basato sull'esperienza maturata in questi anni.

****

02- Sicurezza delle informazioni: la nuova ISO/IEC 27005 sulla valutazione del rischio

Segnalo un mio articolo sulla nuova ISO/IEC 27005 sulla valutazione del rischio: https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-la-nuova-iso-iec-27005-sulla-valutazione-del-rischio/.

Approfondisce quanto avevo già detto in precedenza in altre occasioni.

Come sempre, sono disponibile al confronto nel caso qualcuno voglia discutere le mie posizioni.

****

03- Accreditamento UKAS non più valido per gli appalti pubblici

Il titolo è "Appalti pubblici, Brexit taglia fuori i soggetti accreditati Ukas per le certificazioni": https://ntplusdiritto.ilsole24ore.com/art/appalti-pubblici-brexit-taglia-fuori-soggetti-accreditati-ukas-le-certificazioni-AELxQIND.

La notizia l'avevo vista da un post di LinkedIn di Fabrizio Cirilli (ma il suo link puntava a una pagina del sito del Sole 24 ore con cookie wall), poi me l'ha rimandata Franco Vincenzo Ferrari e allora ho cercato e trovato un link senza cookie wall.

In sostanza: i certificati accreditati da enti non europei non sono reputati validi per partecipare a gare di appalti pubblici. Infatti l'interpretazione dovrebbe riguardare anche i certificati accreditati in Albania, India, USA, Svizzera, eccetera. Non ho indagato se anche gli organismi di accreditamento dello SEE ma non della UE sono esclusi (Islanda, Liechtenstein e Norvegia).

****

04- Security-by-Design and Default Principles del CISA

Ottimo documento del CISA (Cybersecurity and Infrastructure Security Agency degli USA) dal titolo "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default": https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-principles.

In poche pagine (15 in tutto, incluso indice e fuffa introduttiva) sono riportati e spiegati i principi di sviluppo e ingegnerizzazione sicuri.

****

05- Cassazione: assolta Poste Italiane per phishing

Segnalo questo articolo dal titolo "Phishing, perché la Cassazione ha assolto Poste Italiane e condannato i correntisti?": https://www.cybersecitalia.it/phishing-la-cassazione-se-cliente-truffato-la-banca-non-responsabile/24214/.

Ringrazio Maurizio Tardanico che l'ha segnalato su una chat a cui partecipo.

Incollo una parte significativa del testo per dare una prima idea: "la Cassazione ha stabilito che la banca o l'istituto di credito non ha responsabilità nel furto di denaro dei correntisti avvenuto con operazioni di phishing, se ha adottato un sistema di sicurezza tale da impedire a terzi l'accesso al conto corrente e se i clienti stessi hanno fornito i codici di accesso ad estranei, ovviamente, senza esserne consapevoli, perché truffati".

****

06- Sicurezza informatica e Codice degli appalti

Segnalo questo articolo dal titolo "La cyber security entra nel Codice Appalti: perché è un cambio di passo fondamentale": https://www.agendadigitale.eu/sicurezza/la-cyber-security-entra-nel-codice-appalti-perche-e-un-cambio-di-passo-fondamentale/.

Non sapevo che il Codice degli appalti fosse stato cambiato e fosse stata aggiunta questa aggiunta. Poche parole, se ho capito bene, ma molto importanti.

****

07- Privacy: Interpretazione della Corte di giustizia UE su dati pseudonimizzati e anonimi

Segnalo questo post sulla a decisione T-557/20 del 26 aprile 2023 della Corte di Giustizia UE su dati pseudonimi e anonimi: https://www.linkedin.com/posts/maria-grassetto-1a8bb25b_cge-activity-7060175275069779968-LAWc.

Copio biecamente dalla newsletter di Project:IN Avvocati: In estrema sintesi, secondo la Corte occorre ragionare sulla posizione del "ricevente" il dato personale, per indagare sia egli sia - o meno - in grado di identificare il soggetto cui quell'informazione si riferisce, e quindi effettui un "trattamento" di dato personale.

****

08- Privacy: Pagina informativa del Garante sui Dark Pattern

Il The Italian Data Protection Authority ha attivato una pagina informativa sui dark pattern, ossia sulle tecniche per fare in modo che un utente prenda decisioni "inconsapevoli o non desiderate", rinunciando quindi, in ambito privacy, alle limitazioni relative alla raccolta e trattamento dei propri dati personali: https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern.

La pagina fa riferimento alle "Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them" della European Data Protection Board (EDPB), aggiornate a febbraio 2023.

La notizia l'ho letta sulla newsletter di Project:IN Avvocati.

Su questo argomento ero completamente digiuno e questa pagina mi ha aiutato a capire alcune cose. Devo dire che la pagina informativa riassume quanto riportato nelle linee guida dell'EDPB. Queste, invece, approfondiscono le varie tecniche di dark pattern, ma senza esempi concreti e pertanto, in alcuni casi, alcune cose mi sono oscure.

Una versione in italiano dei dark patterns individuati da EDPB è qui: https://www.cyberlaws.it/2022/dark-patterns/.

I dark pattern sono però cose più generali e non riguardano solo la privacy. Ho trovato, per esempio, questo interessante articolo: https://www.drcommodore.it/2018/08/03/dark-pattern-cosa-sono-come-riconoscerli-e-perche-ci-controllano/.

****

09- Privacy: sanzionata la raccolta ingannevole del consenso per marketing

Provvedimento del Garante per "trattamento di dati personali mediante l'uso di pratiche ingannevoli, e in particolare per uso di dark patterns capaci di spingere l'utente a fornire il proprio consenso per finalità di marketing e di comunicazione dei dati a terzi" (ringrazio la newsletter di Project:IN Avvocati per il riassunto): https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014.

Lo segnalo perché è interessante osservare che la raccolta del consenso ingannevole (o forzato, in alcuni casi) è stata sanzionata. Così questo provvedimento mi tornerà utile per convincere qualcuno a fare le cose un po' meglio...

****

10- Gli uomini possono fare tutto (Maggio 2023)

15 maggio. Anche oggi ho iniziato tardi un corso. Accompagno a scuola il piccolo, poi incontro una mamma di un compagno di classe del grande e ci scambiamo idee su come affrontare i compiti. La discussione mi interessa e il tempo passa...

Spero che i partecipanti al corso non mandino un reclamo (il corso finirà mercoledì).

PS: nella foto non ci sono i miei figli.

****

EONL

---

1 Like

Comments

Write a comment...