Infosec & Quality [ITA] - Set. 2023

21 Sept 2023

Monte Ortigara (“Per non dimenticare”). Agosto 2023. Foto mia

Indice

14- ACN e le consulenze gratuite

15- Sentenza sull'uso di Dropbox da parte dei dipendenti (approfondimento)

16- Installazione "pulita" di Windows

17- Chiarimenti EDPB sulle certificazioni GDPR

18- Gli uomini possono fare tutto (Settembre 2023)

****

01- VERA 7.1 ITA e ENG

Per allietare la ripresa estiva di tutti, ho caricato il VERA 7.1 (il mio foglio Excel per il la valutazione del rischio relativa alla sicurezza delle informazioni) in italiano e in inglese sul mio sito: **https://www.cesaregallotti.it/Pubblicazioni.html**.

Il 7.1 in italiano è una correzione del 7.0 già pubblicato, mentre il 7.1 in inglese è la sua traduzione (con l'inglese ero rimasto fermo al 6.0).

Il VERA 7.1 riporta i controlli della ISO/IEC 27001:2013 e quelli della ISO/IEC 27001:2022.

****

02- Interpretazione della NIS2 della Commissione europea

Il 18 settembre ho partecipato, come organizzatore, al convegno di DFA su "NIS 2 e non solo - Aspetti pratici e relazioni". In quella occasione, Pierluigi Perri erri ha fatto riferimento alle "Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)".

Grazie a un post su LinkedIn di Stefano Mele (**https://www.linkedin.com/posts/stefanomele_direttiva-nis2-chiarimenti-applicativi-della-activity-7108489999695642624-Sp9X**) li ho trovati sul web con data di pubblicazione del 14 settembre: **https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive**.

Non li ho ancora letti, ma sicuramente sono interessanti.

****

03- Articolo sullo stato del regolamento DSA

E' evidente che i "nuovi" regolamenti europei mi interessano, almeno per capire il contesto in cui lavoro con la sicurezza delle informazioni. Un articolo che trovo interessante e utile ha titolo "I piani delle big tech per non sgarrare con il Dsa, la nuova legge Ue sul digitale": **https://www.wired.it/article/dsa-google-amazon-tiktok-instagram-facebook-wikipedia-impegni-pubblicita-algoritmi/**.

Sono riassunti gli obblighi più importanti del regolamento DSA è come ci stanno lavorando le aziende più significative.

****

04- Audit degli algoritmi (per Regolamento DSA)

Segnalo questo interessante articolo dal titolo "Audit degli algoritmi: la normativa UE lo prevede, ma non è ancora chiaro come farlo. Ecco perché": **https://www.cybersecurity360.it/legal/audit-degli-algoritmi-la-normativa-ue-lo-prevede-ma-non-e-ancora-chiaro-come-farlo-ecco-perche/**.

Riguarda le grandi piattaforme online e i grandi motori di ricerca, chiamati a identificare i rischi relativi all'uso degli algoritmi di raccomandazione e simili.

L'articolo fa riferimento a una bozza di Delegated regulation (**https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en**). In essa trovo molto interessanti le parti relative agli approcci all'audit e al rischio di audit. Sono approcci che, nell'ambito della sicurezza delle informazioni e dei sistemi di gestione ISO sono rarissimamente utilizzati. Per esempio, viene richiesto di distinguere, come rischi di audit, tra rischi inerenti, rischi di controllo e rischi di rilevazione.

****

05- Articolo sulla Direttiva CER

In questo periodo sono molto attento alle novità normative europee (NIS2, CER, DORA, oltre al GDPR) e alle loro relazioni reciproche. Per questo segnalo (dalla newsletter del Clusit) l'articolo "La nuova direttiva CER riconcilia sicurezza fisica e logica": **https://www.datamanager.it/2023/07/la-nuova-direttiva-cer-riconcilia-sicurezza-fisica-e-logica/**.

L'articolo, come prima cosa, usa il termine "sicurezza cinetica" perché più aggiornato di "sicurezza fisica". Anche qui faccio fatica a capire, ma ritengo utile conoscere i termini usati.

Inoltre chiarisce che "La NIS2 si occupa infatti della sicurezza cyber delle entità critiche e altamente critiche e la CER della loro resilienza rispetto a minacce cinetiche".

****

06- NIST Cybersecurity Framework 2.0 in bozza

Il National Institute of Standards and Technology (NIST) ha pubblicato a inizio agosto la bozza del CSF 2.0: **https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20**.

Si possono mandare commenti al CSF entro il 4 novembre.

****

07- Riferimento pharma per la gestione del rischio

Michaël Hooreman, via LinkedIn, mi ha segnalato il documento "ICH Q9 Quality risk management - Scientific guideline" della European Medicines Agency: **https://www.ema.europa.eu/en/ich-q9-quality-risk-management-scientific-guideline**.

Il documento presenta approcci di valutazione del rischio che possono essere usati nell'ambito della qualità. A mio parere non solo, perché potrebbero essere benissimo applicati, con qualche aggiustamento, anche alla sicurezza delle informazioni e forse ad altri campi. In tutti i casi, visto che si tratta di approcci validi e diffusi, sarebbe opportuno che chi si occupa di sicurezza delle informazioni li conoscesse, per evitare di fossilizzarsi su un solo modello.

Utile anche per quanto riguarda la sola qualità per capire meglio gli ambiti di applicazione della valutazione del rischio. A mio parere, la ISO9001, con l'ultima edizione basata sull'HLS, non è molto chiara sull'ambito di applicazione della gestione del rischio (problema riscontrabile su tutte le norme sui sistemi di gestione). Leggendo il testo con tanta attenzione, si trova che la gestione del rischio dovrebbe riguardare solo l'efficacia del sistema di gestione (e quindi trattare solo rischi gestionali), ma molti l'applicano per i rischi più operativi e questo non è necessariamente un male. Questo documento permette di approfondire, seppur sinteticamente, questi aspetti.

****

08- Riconoscere le minacce deepfake

National Security Agency, Federal Bureau of Investigation (FBI) e Cybersecurity and Infrastructure Security Agency hanno pubblicato un breve (18 pagine) rapporto dal titolo "Contextualizing Deepfake Threats to Organizations": **https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats**.

Scritto bene e sintetico, spiega cosa sono queste minacce.

Un capitolo spiega perché le minacce deepfake possono avere impatti sulle organizzazioni (attaccare l'immagine di persone collegate all'organizzazione, capacità di impersonare qualcuno e quindi frodare qualcuno o avere accesso a dati o sistemi). Si tratta di casi forse rari per molti, ma sicuramente da considerare.

Le contromisure sono legate alla capacità di ciascuno di analizzare il materiale potenzialmente alterato.

****

09- Whitepaper di ISC2 sulla business continuity

Segnalo che ISC2 ha pubblicato il documento "La Business Continuity", che illustra i passi da fare per affrontare questo argomento: **https://www.isc2chapter-italy.it/nuovo-whitepaper-sulla-business-continuity/**.

Il taglio è didattico e ben fatto.

Ero stato informato della preparazione del documento e ne avevo letto la bozza. Ringrazio invece Franco Vincenzo Ferrari zo Ferrari per avermene segnalato la pubblicazione.

****

10- Capitolati di gara e requisiti di sicurezza IT

Chiara Ponti ha segnalato un articolo dal titolo "Quali i requisiti di cyber security nei capitolati di gara? Analisi del report condotto da R. Setola con Unindustria, Centro di Competenza Cyber 4.0 e AIPSA": **https://www.cybersecitalia.it/quali-i-requisiti-di-cyber-security-nei-capitolati-di-gara-analisi-del-report-condotto-da-r-setola-con-unindustria-centro-di-competenza-cyber-4-0-e-aipsa/25838/**.

L'indagine ha coinvolto 32 aziende. Dall'elenco iniziale del report di grande o grandissima dimensione. Quindi i risultati vanno analizzati in quest'ottica.

La lettura del documento è comunque utile per ripassare le misure di sicurezza che possono essere chieste ai fornitori (io dovrò quindi aggiornare la mia lista).

****

11- Social e codice etico dei dipendenti pubblici

Il DPR 62 del 2013 reca il codice di comportamento dei dipendenti pubblici. Con il DPR 81 del 2023 sono stati inseriti aspetti relativi all'uso dei social media. Per questo rimando all'articolo su Altalex: **https://www.altalex.com/documents/news/2023/07/11/codice-etico-dipendenti-pubblici-novita-email-social-media-inclusione**.

Gli elementi introdotti, che quindi confronterò con quanto da me fatto in passato:

- l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa;
- l'utilizzo di email personali è di norma evitato per attività di servizio, tranne nel caso in cui non si possa accedere all'account istituzionale;
- il dipendente è responsabile del contenuto dei messaggi inviati;
- i dipendenti si uniformano alle modalità di firma dei messaggi indicate dall'amministrazione di appartenenza;
- ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile;
- al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali;
- è vietato l'invio di email che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.
- nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza;

- il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.
- le comunicazioni, afferenti direttamente o indirettamente il servizio, non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media.

****

12- Sanità: attacchi IT e sicurezza dei pazienti

Sandro Sanna mi ha segnalato la pubblicazione Sentinel Event Alert 67 dal titolo "Preserving patient safety after a cyberattack": **https://www.jointcommission.org/resources/sentinel-event/sentinel-event-alert-newsletters/sentinel-event-alert-67-preserving-patient-safety-after-a-cyberattack/**.

Una lettura interessante, anche se in troppi punti ripete cose note e vaghe (costituite un comitato, designate un gruppo di risposta, fate formazione). Interessante anche perché dimostra la necessità di analizzare i tanti casi che possono presentarsi in un'azienda ospedaliera e le tante possibili soluzioni, non necessariamente informatiche.

****

13- ACN e le consulenze gratuite

Francesca Nobilini ha scritto un post su LinkedIn su Agenzia per la Cybersicurezza Nazionale che cerca collaborazioni gratuite: **https://www.linkedin.com/posts/francesca-nobilini_lavora-con-noi-activity-7099309386753306624-jfEy**.

Molti, in effetti, si lamentano del fatto che non si tratta certamente di una proposta etica. Aggiungerei anche che il rischio è che "Ciò che costa poco vale anche poco" (frase che trovo attribuita, in italiano, a Baltasar Graciàn, ma che non trovo in spagnolo). Su questo sono molto dispiaciuto di come ACN dimostra di valutare il nostro lavoro.

Dico che essere contattati da ACN per un supporto o un chiarimento sarebbe un onore, così come essere invitati a giornate di studio o convegni. Un impegno non eccessivo e una bella visibilità, oltre alla possibilità di confrontarsi e approfittare della giornata di studio. Questo è quello che facciamo abitualmente e gratuitamente. Ma così come proposto è decisamente poco allettante (e, ripeto, un segnale di scarsa considerazione).

Peccato. Spero in un cambiamento.

****

14- ACN, le regole per i servizi cloud e il rispetto "per chi lavora"

Franco Vincenzo Ferrari mi ha segnalato che su Agenzia per la Cybersicurezza Nazionale ha aggiornato i termini della qualificazione dei servizi cloud per la Pubblica Amministrazione: **https://www.acn.gov.it/notizie/contenuti/cloud-acn-aggiorna-i-termini-della-qualificazione-dei-servizi-per-la-pubblica-amministrazione**.

Niente di troppo significativo, a meno che non siate fornitori della PA.

E' comunque il caso di NON ringraziare ACN per:

- continuare a mettere a disposizione documenti in pdf non editabili, così da impedire il copia-incolla e far perdere tempo alle organizzazioni che devono aggiornare le proprie check list e i propri documenti;
- non aver prodotto il consolidato delle misure da adottare (l'allegato alla Determina 307 del 2023).

****

15- Sentenza sull'uso di Dropbox da parte dei dipendenti (approfondimento)

Avevo scritto a luglio di una sentenza sull'uso di Dropbox da parte dei dipendenti (**http://blog.cesaregallotti.it/2023/07/sentenza-sulluso-di-dropbox-da-parte.html**).

A questo proposito, segnalo un articolo di approfondimento, segnalatomi da Stefano Gazzella dal titolo "Disciplinare l'impiego dei servizi di condivisione in cloud per ridurre i rischi legali": **https://www.redhotcyber.com/post/disciplinare-limpiego-dei-servizi-di-condivisione-in-cloud-per-ridurre-i-rischi-legali/**.

****

16- Installazione "pulita" di Windows

Segnalo questo articolo dal titolo "Windows 11 has made the "clean Windows install" an oxymoron": **https://arstechnica.com/gadgets/2023/08/windows-11-has-made-the-clean-windows-install-an-oxymoron/**.

Il punto è questo: tutti i produttori di hardware, quando vendono il pc con il sistema operativo incluso, lo fanno con una versione piena di software aggiuntivi spesso inutili se non dannosi (riducono le prestazioni, lo spazio disco e anche la concentrazione dell'utente). Quindi molti installano una versione "pulita" di Windows e questa tecnica prende il nome di "clean Windows install".

Purtroppo, anche prima di Windows 11 a guardare con attenzione, lo stesso Windows non è "pulito" e installa numerosi software inutili (o, meglio, dannosi).

Ormai lo dicono tutti e lo ripeto: i grandi dell'informatici ormai stanno usando i propri prodotti e servizi per venderci sempre più roba e raccogliere sempre i nostri dati (per venderci roba o venderli ad altri che vogliono venderci roba). Forse un po' il regolamento DSA limiterà l'impatto, ma la direzione è quella da molto tempo e possiamo solo prenderne atto e difenderci come possiamo (a meno di non accettare di essere infelici così come lo siamo per gli effetti del consumismo... ma questi sono temi per filosofi, non per miseri consulenti come me).

****

17- Chiarimenti EDPB sulle certificazioni GDPR

European Data Protection Board, il 1 agosto, ha risposto a una richiesta di chiarimenti di Accredia in merito alla certificazioni GDPR (mi si permetta di usare questa espressione): **https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-accredia_en**.

Ringrazio la newsletter Project:IN Avvocati per la segnalazione.

La risposta è molto tecnica e ho dovuto leggerla tre volte per capirla (posso sempre dire che il periodo è vacanziero...) e vorrei segnalare alcuni punti per me significativi, più per gli organismi di certificazioni che sulle organizzazioni che intendono certificarsi:

- EDPB ribadisce che il suo compito è valutare i criteri di certificazione, non le attività di accreditamento, anche nel caso di sigilli europei sulla protezione dei dati (European Data Protection Seal), che sono invece in carico ai Garanti dei singoli Stati membri;
- deve essere stabilito uno "scheme owner", anche perché richiesto dalla ISO/IEC 17065, che può essere anche un organismo di certificazione accreditato (nel caso di Europrivacy, lo scheme owner è Europrivacy stessa); penso che sia chiaro che un organismo di certificazione che lavora da solo rilascerebbe però certificazioni che potrebbero risultare meno interessanti di certificazioni comuni ad altri, come minimo perché si avrebbe una maggiore visibilità;
- gli organismi di certificazione possono quindi adottare, nel caso di Europrivacy, i criteri di Europrivacy per essere accreditati dal proprio garante nazionale (o, se il caso, dal proprio organismo di accreditamento).

Infine, a me sembra di capire che l'accreditamento debba essere dato per ciascuno stato dove l'organismo di certificazione opera dal relativo garante nazionale (o, se il caso, dal proprio organismo di accreditamento); questo diventerebbe pesante perché un organismo di certificazione che vuole lavorare nei 27 Stati della UE deve avere 27 accreditamenti, a cui forse aggiungere gli altri 3 Paesi del SSE (chiedo aiuto a chi mi sa rispondere) e non voglio pensare al fatto che la Germania ha in realtà ha più garanti privacy; ma su questo c'è un invito di EDPB a EA per considerare come un organismo di accreditamento nazionale possa collegarsi a più Garanti. Però Giovanni Francescutti cutti di DNV mi ha contraddetto su LinkedIn. Confesso la mia confusione.

Direi che come mal di testa da rientro dalle vacanze siamo a posto.

****

18- Gli uomini possono fare tutto (Settembre 2023)

Rientro un po' impegnativo. Pensavo di poter evitare di controllare le chat WhatsApp di mio figlio dodicenne (il decenne non ha ancora il cellulare). Invece ho scoperto che i compagni mandano di tutto. Alcuni inviano centinaia di gif, tra queste ho visto anche bestemmie e una decapitazione (forse da un video dell'Isis). Poi alcuni inseriscono altri, senza chiedere il permesso, in altri gruppi di centinaia di persone.

Alcune cose sono sicuramente materia di buona educazione (evitare di mandare troppa roba nelle chat, evitare di inserire persone nelle chat), altre rappresentano rischi (diffondere il

numero di telefono di altri), altre ancora riguardano l'incapacità di discernimento propria dei giovanissimi che va tutelata.

L'unica arma è stata quella di contattare i genitori di alcuni compagni di mio figlio. Fortunatamente persone civili che hanno capito immediatamente il senso della comunicazione.

****

EONL