Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – MAGGIO 2019

****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque.

E' disponibile il blog http://blog.cesaregallotti.it.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy: http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****

Indice

****

01- ITIL 4 Foundation

Axelos (la società che mantiene ITIL) da tempo aveva annunciato la pubblicazione prevista per il 2019 di ITIL 4, ossia la nuova edizione di ITIL (ricordo che la precedente edizione era la ITIL 2011, a sua volta un aggiornamento minore di ITILv3 e segnalo che si divertono molto a cambiare il modo di indicare le versioni):
- https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

Interessante il fatto che al momento non risulta pubblicato ITIL 4, per lo meno come lo intenderemmo dopo aver visto i 5 (non agili) volumi di ITILv3 e ITIL 2011. Risulta pubblicato solo il manuale per sostenere l'esame ITILv4 Foundation.

L'esame è disponibile dal 28 febbraio:
- https://www.axelos.com/certifications/itil-certifications/itil-foundation-level.

Da quanto è scritto sul sito di Axelos, ITILv4 ruoterà interno al concetto di "sistema del valore del servizio" (service value system, SVS) e si concentrerà sulla "co-creazione del valore attraverso le relazioni determinate dal servizio". Il SVS rappresenta come i componenti e le attività possono lavorare insieme per facilitare la creazione del valore attraverso i servizi.

Tanti bei paroloni (appare, ma non l'ho riportato, anche "olistico", che è un indicatore del livello di fuffa di un testo). Però, dopo aver letto il manuale, posso dire che mi è piaciuto. Il primo motivo è perché è breve e mette già a disposizione le informazioni di base del modello ITIL, senza doverle estrarre da volumi più ampi. Il secondo motivo è perché tecnicamente è molto più convincente, coerente e utile delle ultime 2 versioni (ITILv3 e ITIL 2011). Riporto quindi nel seguito i miei appunti sulle parti tecniche.

Ora il modello ruota intorno a 3 elementi chiave: le attività del SVS (Service value system), le pratiche e i principi.

Le attività del SVS sono 6: pianificazione, miglioramento, coinvolgimento (engage), progettazione (design) e transizione, ottenimento o realizzazione, consegna e supporto (in precedenza, ITIL ruotava intorno alle 5 fasi di strategia, progettazione, transizione, esercizio, miglioramento continuo).

Sono anche trattate le 4 "dimensioni della gestione dei servizi", ossia le vecchie 4 P, anche se con nome leggermente diverso.

Le "pratiche" corrispondono ai "processi" delle precedenti versioni. Sono 34 divise in generali, di servizio e tecniche. Si vede quindi che non sono diminuite. L'idea è però quella di fornire indicazioni in merito agli aspetti della gestione dei servizi, non di presentare un modello unitario e coerente di queste pratiche. Mi permetto di tradurre così: dopo averci tormentati con i processi e la loro importanza, dopo averne creati troppi, dopo non essere riusciti a diminuirli, gli autori di ITIL hanno rinunciato a dare una visione dei processi come sistema (ossia a correrlarli tra loro) e li hanno chiamati "pratiche".

Se pure molte indicazioni sono interessanti, è in effetti difficile capire le relazioni tra le pratiche di "service design" e "change control" (non mi pare siano spiegate) e tra le pratiche di "release management" e "deployement management" (anche se per queste è fornita una spiegazione).

Sulle pratiche, segnalo poche cose:
- rinuncia al termine "risorse umane" per "forza lavoro e talenti" (workforce and talent);
- sottolinea che il CMS (configuration management system) è importante, ma non è necessario che sia di dettaglio e che è possibile averne più di uno (questo ricordando certi consulenti che promuovono un unico CMS o CMDB o Asset inventory, evidentemente senza avere idea di cosa sono veramente);
- ricorda che i processi di controllo dei change possono essere distinti per ambienti distinti (in molti pensavano ad un unico change manager per tutti i change);
- rinuncia (per lo meno a livello di foundation) al change manager e al CAB (change advisory board), ricordando solo che vanno previsti diversi livelli di autorizzazione per i change;
- riduce notevolmente l'importanza della pratica di "change control" rispetto a quanto in precedenza era importante il processo di change management (lo cita solo una volta nei 4 esempi forniti in Appendice A);
- usa il termine "continuity" per eventi di elevato impatto, contrariamente ad altri (per esempio il BCI) che invece lo usa anche per incidenti di impatto minore.

Per ogni pratica, sono indicati gli impatti sulle 6 attività del SVS. Questo punto spesso non mi è risultato chiaro e, anzi, alcune relazioni non mi hanno trovato d'accordo. Si tratta sicuramente di un tentativo di

correlare il modello SVS con le 36 pratiche. Come spesso succede, i tentativi di correlare modelli diversi risultano difficili e il risultato non è buono.

I principi sono 8. Sono trattati all'inizio e poi quasi dimenticati. Di questi, anche come conclusione di questa analisi superficiali, vorrei ricordarne 3:
- il primo è la promozione della "progressione iterativa con riscontri" ossia dell'approccio Agile, criticando, in qualche modo, chi ha cercato di adottare ITIL con un approccio di reingenierizzazione dei processi (si ritorna, insomma, al Kaizen promosso nell'ambito della qualità);
- il secondo è di "partire da dove si è", ossia di essere consapevoli del proprio stato prima di iniziare attività di miglioramento; questo lo ricordo perché include, finalmente, una critica alle misurazioni e un richiamo all'importanza del monitoraggio;
- il terzo principio che ricordo è quello di "rendere semplice e pratico", spesso dimenticato da manager, consulenti e auditor; la frase che mi sono segnato è: "Simplicity is the ultimate sophistication".

Ora dovrò sostenere l'esame. Le differenze rispetto a ITIL 2011 sono molte e molti consigliano di seguire il corso completo. Io ho preferito studiare da solo il manuale. Spero di non aver fatto una scelta sbagliata.

****

02- Mia intervista per Coretech

CoreTech, nella persona di Roberto Beneduci (Founder & CEO), mi ha invitato a tenere un intervento al suo convegno annuale (CoreTech Summit) sul tema della business continuity.

Mi hanno quindi fatto un'intervista "preventiva" pubblicata su LinkedIn. Per chi vuole ascoltarmi (e ascoltare anche Roberto) per poco più di 12 minuti, il link è questo (mi pare che questo video sia visibile anche senza accedere a LinkedIn):
- https://www.linkedin.com/feed/update/urn:li:activity:6531774727407562752.

****

03- Standard: ISO/IEC 27050-2 su electronic discovery

Seppur con grande ritardo, segnalo che a settembre 2018 è stata pubblicata la ISO/IEC 27050-2:2018 dal titolo "Information technology -- Electronic discovery -- Part 2: Guidance for governance and management of electronic discovery":
- https://www.iso.org/standard/66230.html.

Non mi pare aggiunga alcunché a quanto già noto, visto che è soprattutto una norma di tipo "gestionale" e non tecnico.

In sostanza, senza fornire molti dettagli, dice di prevedere regole in merito a: archiviazione, identificazione delle prove, dichiarazioni e comunicazione, gestione del rischio, monitoraggio e rendicontazione.

****

04- Standard: EN 50600 e ISO/IEC TS 22237 per i data center (mio articolo)

Ho scritto un breve articolo di compilazione sullo standard ISO/IEC TS 22237 sui data center. Si tratta, se posso semplificare e quindi essere criticato, della "risposta europea" al "Tier Standard: Topology" dell'Uptime Instititue e all'ANSI TIA-942.

Infatti la ISO/IEC TS 22237 nasce dalle norme europee EN 50600.

Il mio articolo:
- https://www.ictsecuritymagazine.com/articoli/gli-standard-en-50600-e-iso-iec-ts-22237-per-i-data-center/.

****
05- ENISA Maturity Evaluation Methodology for CSIRTs

L'ENISA ha pubblicato un documento dal titolo "ENISA Maturity Evaluation Methodology for CSIRTs" (è l'aggiornamento di un documento del 2017):
- https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process.

Non mi piacciono molto i modelli di maturità, questo dà comunque indicazioni utili per costruire un computer security incident response team (ricordo, a questo proposito, anche la guida dell'ETSI per costruire un SOC, di cui avevo scritto a suo tempo: http://blog.cesaregallotti.it/2019/01/guida-etsi-per-un-soc.html).

****
06- Legale: Controllo dei lavoratori, Statuto lavoratori, penale e civile

Franco Vincenzo Ferrari di DNV GL Business Assurance Italia mi ha segnalato un articolo dal titolo "Cassazione penale: utilizzabili le riprese di un impianto di video-sorveglianza non conforme alla normativa privacy":
- https://www.forensicsgroup.eu/2019/05/cassazione-penale-utilizzabili-le-riprese-di-un-impianto-di-video-sorveglianza-non-conforme-alla-normativa-privacy/.

Si tratta di una sentenza della Cassazione, per cui si possono usare in un processo penale delle prove raccolte da strumenti di monitoraggio non coerenti con l'art. 4 dello Statuto dei lavoratori. Infatti questo riguarda il diritto privato e non il penale.

****
07- CSA IoT Security Controls Framework

Il Cloud Security Alliance (CSA) ha pubblicato una lista di misure di sicurezza da prevedere per l'IoT dal titolo "CSA IoT Security Controls Framework":
- https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework.

Questa lista è accompagnata da una guida "CSA Guide to the IoT Security Controls Framework":
- https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/.

Per scaricare i documenti è necessario registrarsi (ma è possibile farlo anche usando dati totalmente inventati).

Il tutto sembra destinato soprattutto a organizzazioni che vogliono usare dispositivi IoT.

La lista non è certo agile, visto che si tratta di 160 controlli. Il suo utilizzo richiede la capacità di adattarla alle proprie esigenze (io, per esempio, trovo eccessivamente numerosi i controlli dedicati alla valutazione del rischio; però sono contento che alla gestione degli incidenti siano dedicati solo 2 controlli). Può comunque essere utile a chiunque voglia produrre o usare dispositivi o sistemi per l'IoT.

La notizia l'ho vista inoltrata da un post di LinkedIn di Laura Zarrillo (che a sua volta ha fornito un link di continuitycentral.com). Per vederlo è necessario essere iscritti a LinkedIn:
- https://www.linkedin.com/feed/update/urn:li:activity:6528994891962425344

****

08- Bollettino MELANI 2/2019

Il rapporto semestrale della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI (della Confederazione Svizzera) è a mio parere uno dei documenti più interessanti. Segnalo quindi il rapporto relativo alla seconda metà del 2018, uscito in questi giorni:
- https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/melani-halbjahresbericht-2-2018.html.

I temi "caldi" sono l'IoT, la «fake sextortion» e la compromissione delle utenze di Office 365.

****

09- Microsoft e il cambio delle password

Sul SANS NewsBites del 26 aprile trovo la notizia che Microsoft riconosce l'inutilità di forzare il cambio delle password:
- https://blogs.technet.microsoft.com/secguide/2019/04/24/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903/.

Questo in realtà si trova in un'idea per la prossima versione delle Security baselines di Windows: non avere più come default la richiesta di cambio periodico delle password.

Questa posizione è la stessa assunta dal NIST quasi due anni fa e di cui avevo già parlato all'epoca:
- http://blog.cesaregallotti.it/2017/08/del-nist-e-della-lunghezza-e.html.

Ricordo che "si ritiene preferibile lasciare liberi gli utenti di scegliere le proprie password, purché di almeno 8 caratteri e non presenti in una blacklist di password troppo facili". Purtroppo non sembra che i futuri sistemi Windows automatizzeranno queste blacklist. Anzi, il post di Microsoft dichiara che è compito degli utilizzatori realizzare le blacklist o meccanismi di autenticazione a più fattori (multi-factor authentication).

Di primo acchito, non mi pare un miglioramento (sappiamo quanto siano spesso superficiali molti amministratori di sistema; semplicemente non attueranno niente di più di quello previsto dalle baseline). Inoltre mi lascia sempre perplesso l'assenza di riflessioni sull'abitudine di molti utilizzatori aziendali di scambiarsi le password e delle possibili contromisure alternative al cambio periodico delle password. C'è però la riflessione sul fatto che oggi i sisitemi MFA, con la diffusione degli smartphone, siano sempre più economici e facili da usare.

****