PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5196 di Venerdì 01 luglio 2022

# Protezione dei dati: ecco una bozza di norma preziosissima!

***Il comitato ISO / TC 292 "security and resilience" ha cominciato a lavorare su una bozza di norma, che potrà permettere a titolari e responsabili della protezione dei dati di elaborare linee guida per la messa in sicurezza di documenti fisici.***

Ricordo ai lettori che un gruppo di lavoro specializzato di questo comitato tecnico già da tempo ha pubblicato alcune norme, che riguardano le garanzie di autenticità, integrità e affidabilità di prodotti e documenti. Ad esempio, queste norme risultano preziose per proteggere i prodotti di grandi marche da sempre più frequenti contraffazioni.

Quest'ultima bozza di norma è dedicata in particolare alla elaborazione di linee guida per la messa in sicurezza di documenti fisici. È evidente come il trattamento di dati personali e la protezione dei supporti cartacei, sui quali si trovano in dati personali, siano attività direttamente coinvolte in queste linee guida.

I sempre più frequenti i casi di data breach, con tutte le conseguenze che i titolari coinvolti ben conoscono, dovrebbero costituire un ulteriore incentivo a studiare attentamente queste linee guida e vedere di attuare indicazioni, che per il codice civile italiano corrispondono a regola d'arte.

Vediamo i temi affrontati e le soluzioni proposte.

Siamo tutti d'accordo che ancora oggi i documenti cartacei svolgono una funzione fondamentale nell'ambito di transazioni economiche, legali e sociali, in quanto costituiscono la base per titoli di proprietà, per verifica di identità, per conferma dei titoli accademici, per abilitazione alla guida e via dicendo.

Queste funzioni critiche fanno sì che questi documenti possano essere un attraente bersaglio per la contraffazione, l'alterazione ed altre forme di frode, che portano a diminuire l'affidabilità di questi documenti ed a creare problemi non indifferenti ai soggetti coinvolti.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

L'obiettivo di questa norma internazionale è quella di determinare inizialmente quali siano i livelli di rischio, a fronte dei più tipici scenari di attacco, e successivamente di proporre delle linee guida sulla messa in sicurezza dei documenti in causa.

Naturalmente i rischi cambiano nel tempo e diventa difficile, per una norma, essere costantemente aggiornata. Ecco il motivo per cui gli elaboratori della norma si sentono in dovere di mettere in evidenza, sin dal primo paragrafo, quali siano i rischi che non sono presi in considerazione in questo documento:

- i rischi tecnici, che nascono dal fatto che gli strumenti di sicurezza non sono applicati in modo corretto,
- i rischi di gestione, connessi al fatto che i documenti possono essere state esaminati da persone non autorizzate,
- i rischi organizzativi, che comportano la raccolta di dati presenti sui documenti esaminati o un'analisi non sufficientemente approfondita di possibili indizi di alterazione,
- i rischi di origine esterna, ad esempio la mancanza di rete o danneggiamenti di apparecchiature,
- infine, non vengono prese in considerazione i rischi di mancata conformità a leggi e regolamenti.

Ciò premesso, vediamo di che cosa la norma si occupa:

-viene condotta inizialmente una valutazione di rischio, che permette di determinare a quale classe di rischio appartiene il documento, che deve essere protetto.

Si passa quindi ad illustrare una panoramica delle possibili misure di sicurezza, seguita da una valutazione del rapporto fra queste misure ed il livello di protezione richiesto dal documento.

Infine, si esamina il nuovo livello di rischio, conseguente a queste azioni di mitigazione.

Resta inteso che questo documento non si applica a banconote, documenti di viaggio, francobolli, carte di identità nazionale ed altri documenti, per i quali esistono già normative garantistiche.

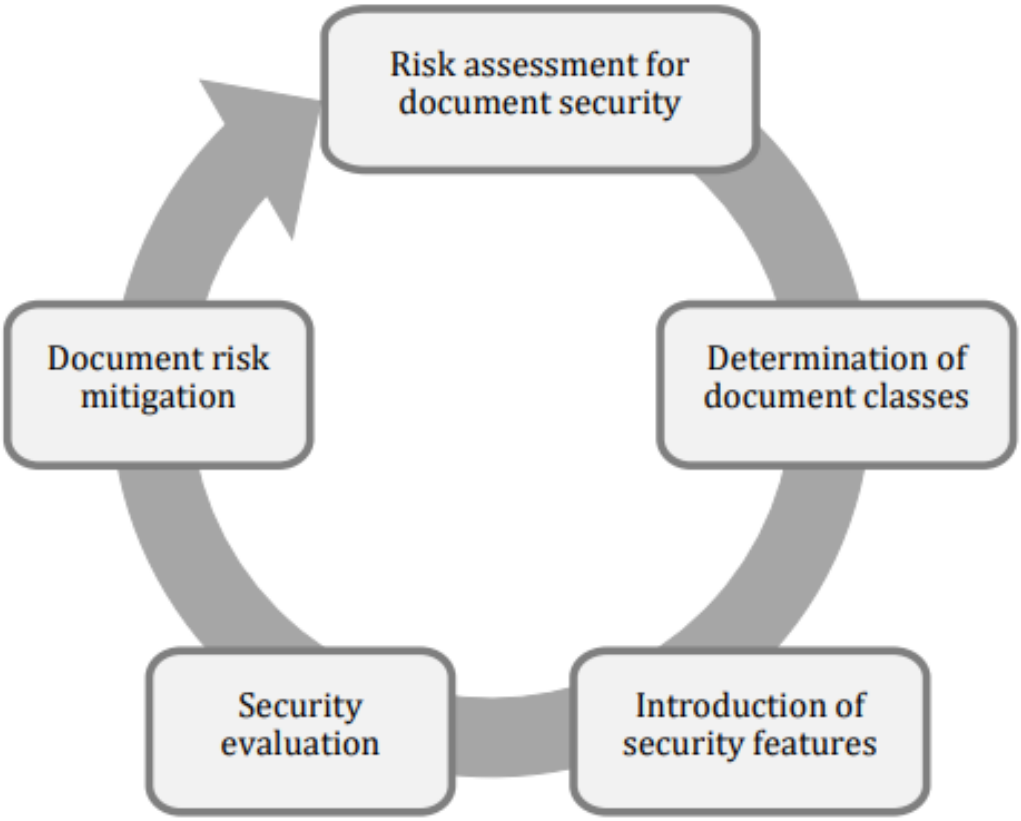
Un aspetto molto interessante, che viene preso in considerazione della norma, riguarda il profilo di competenza professionale del soggetto che deve fisicamente esaminare il documento, per valutarne la genuinità.

Si tratta di un aspetto estremamente critico, anche perché non basta che il soggetto abbia una specifica competenza; occorre anche che esso abbia a disposizione eventuali specifici strumenti e anche il tempo necessario per poterli analizzare.

Si tratta di un aspetto spesso trascurato, che invece ha un ruolo fondamentale, per attribuire ad appropriati soggetti appropriate responsabilità. Si pensi ad esempio ad un addetto ad un punto di accoglienza, che avrà a disposizione sì e no alcuni secondi per esaminare un titolo di accesso, mentre un laboratorio criminologico può avere a disposizione giorni e giorni di esame, con l'utilizzo di sofisticatissime apparecchiature.

Pretendere lo stesso livello di competenza nell'analisi, in questi due diversi scenari, rappresenta evidentemente una inaccettabile forzatura.

Secondo lo schema ormai ben noto, chiamato con l'acronimo P-D-C-A, la norma illustra la procedura per la messa a punto di un progetto di messa in sicurezza di un documento.




È uno schema che i lettori ben conoscono e che viene ormai utilizzato nella gran parte dei documenti, destinati all'analisi di rischio ed alla messa sotto controllo del rischio stesso.

La norma prosegue mettendo in evidenza quali sono le quattro principali tecniche di attacco, cui documenti possono essere soggetti:

- la clonazione, vale a dire la riproduzione acribica di un documento originale,
- il facsimile, vale a dire una riproduzione non autorizzata del documento originale, nella quale qualche caratteristica di sicurezza può essere omessa,
- l'alterazione, laddove vengono introdotte delle modifiche ad un documento genuino, come ad esempio cambio della fotografia od altro,
- il furto di specifici elementi di sicurezza, vale a dire la capacità di riprodurre caratteristiche di sicurezza originali, grazie alla acquisizione illecita di queste caratteristiche.

Infine la norma classifica i documenti in tre categorie, che vanno dall'alto rischio, al rischio moderato, fino ai documenti a basso rischio.

Successivamente la norma illustra le numerose tecnologie di sicurezza che possono essere utilizzate e che portano a definire il nuovo livello di rischio del documento originale.

Una serie di allegati offre tutta una serie di esempi, con il calcolo del livello di rischio residuo, in funzione delle misure di sicurezza adottate.

In sintesi, un documento preziosissimo che permetterà ai responsabili della protezione di dati personali, su supporto cartaceo, di adottare tecnologie protettive conformi alla regola d'arte!

**Adalberto Biasiotti**

 Licenza Creative Commons

---

**www.puntosicuro.it**