	detentore della password la smarrisca o lasci l'organizzazione. - Contro: occorre affidarsi a un soggetto fidato.
References	- Rimuovere o reimpostare le password dei file in Office, https://docs.microsoft.com/it-it/previous-versions/office/office-2013-resource-kit/jj923033(v=office.15)?redirectedfrom=MSDN

5.9.4 Procedure

A i principi generali già introdotti nel paragrafo [rif. 5.1.7], si aggiungono le seguenti indicazioni per il contesto specifico:

Patching	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Per quanto concerne il Patching, il Microsoft Security Response Center rilascia mensilmente dei bollettini sulla sicurezza che descrivono gli aggiornamenti di sicurezza pubblicati nel mese corrente. Essi risolvono le vulnerabilità legate alla sicurezza del software Microsoft, i relativi rimedi e forniscono i collegamenti agli aggiornamenti applicabili per il software interessato.
References	- Security Bulletins, https://docs.microsoft.com/en-us/security-updates/securitybulletins/securitybulletins

Procedura	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Visto che: A partire da Office 2013 si distinguono 2 tipi di documenti: "normal" e "macro-enabled": - Normal (default): .docx, .xlsx e .pptx - Macro-enabled: .docm, .xlsm, .pptm I documenti "normal" ('x') non hanno macro abilitate, mentre i documenti "macro-enabled" hanno le macro abilitate La regola più sicura è che si dovrebbe usare sempre documenti di tipo "normal" ('x' finale), evitando di aprire quelli contenenti macro.

5.9.5 References and additional information

I riferimenti sono già stati riportati all'interno delle singole best practices.

5.10 Sicurezza del pacchetto OpenOffice

5.10.1 Hardening

Hardening della suite OpenOffice	
Minaccia	- Accesso non autorizzato alle informazioni.

	- Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Limitare/Disabilitare/Condizionare l'uso di contenuti attivi. Per contenuti attivi si intendono: - EXE, COM, PIF, SCR, etc.: Binary code; - BAT, CMD, VBS, JS, etc.: Commands, Scripts; - HTML, XML, XHTML: Scripts; - PDF: Scripts, Embedded files, Commands - Word, Excel, PowerPoint, Access, … : Macros, OLE objects, Embedded files, Commands; - URLs. OpenOffice offre una certa difesa a livello di: - esecuzione delle macro (4 modalità -low, medium, high, very high- e possibilità di definizione di "trusted sources"); - navigazione degli hyperlinks (attraverso Ctrl-click).
References	- Security options, https://wiki.openoffice.org/wiki/Documentation/OOo3_User_Guides/Getting_Started

Hardening della suite OpenOffice	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	I documenti possono contenere grandi quantità di informazioni nascoste: - Nome utente, organizzazione; - Storia delle modifiche, aggiunte, cancellazioni; - Note, Commenti; - Testo nascosto; - Un intero foglio di calcolo "dietro" a un semplice diagramma (con cifre aziendali confidenziali!) ; - A volte anche blocchi casuali di memoria. Se si registrano le modifiche al documento o si includono informazioni o commenti nascosti nei documenti, per evitare la diffusione incontrollata di tali informazioni utilizzare i meccanismi messi a disposizione da OpenOffice che consentono di: - impostare warnings per ricordare (in fase di firma, esportazione PDF e salvataggio) di rimuovere tali informazioni oppure; - rimuovere automaticamente alcune informazioni.
References	- Security options and warnings, https://wiki.openoffice.org/wiki/Documentation/OOo3_User_Guides/Getting_Started

Hardening del sistema operativo che ospita la suite OpenOffice	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Eseguire l'hardening del sistema operativo che ospita la suite [rif. 5.2.2]. Installare sul sistema software anti-malware in grado di: - analizzare i "contenuti attivi" presenti nei documenti OpenOffice rilevando la presenza di malware; - rimuovere dai documenti OpenOffice i "contenuti attivi" in base a specifiche