	Installare sul sistema software anti-malware in grado di: - analizzare i "contenuti attivi" presenti nei documenti Office rilevando la presenza di malware; - rimuovere dai documenti di Office i "contenuti attivi" in base a specifiche politiche configurabili, ad es. In base alla tipologia (macro, scripts, oggetti "embedded", applets, etc.), e altre caratteristiche.

5.9.2 Autorizzazione

A i principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Proteggere i parametri di sicurezza e la definizione delle "trusted location" da eventuali cambiamenti apportati dagli utenti finali. Tali configurazioni devono essere impostabili solo da un'utenza amministrativa.

5.9.3 Crittografia

A i principi generali già introdotti nel paragrafo [rif. 5.1.4], si aggiungono le seguenti indicazioni per il contesto specifico:

Crittografia	
Minaccia	- Accesso non autorizzato alle informazioni - Attacchi all'integrità delle informazioni. - Falsificazione di identità.
Contromisure	Si tengano presenti i seguenti strumenti integrati in Office: - L'utilizzo di firma digitale per la protezione dell'integrità dei documenti prodotti (Gli utenti possono firmare digitalmente un documento di Excel, PowerPoint o Word); - L'utilizzo di meccanismi per la protezione della confidenzialità dei documenti prodotti eseguendone la cifratura. Sono disponibili impostazioni che consentono di imporre l'utilizzo di password complesse, ad esempio regole relative alla complessità e alla lunghezza.
References	- Pianificare le impostazioni della firma digitale per Office 2013, https://docs.microsoft.com/it-it/previous-versions/office/office-2013-resource-kit/cc545900(v=office.15)?redirectedfrom=MSDN - Pianificare le impostazioni di complessità delle password per Office 2013, https://technet.microsoft.com/it-it/library/ff657853.aspx

Crittografia	
Minaccia	Disponibilità dei servizi.
Contromisure	Valutare l'adozione dello strumento DocRecrypt che funziona sul principio del Key escrow, ovvero un accordo in cui le chiavi necessarie per decifrare i dati crittografati sono detenuti in un "deposito" (escrow) in modo che, in determinate circostanze, una terza parte autorizzata, ad esempio un apposito incaricato appartenente alla Security dell'organizzazione, possa accedere a tali chiavi. - Pro: si può recuperare il contenuto di un file cifrato anche nell'eventualità che il