	politiche configurabili, ad es. In base alla tipologia (macro, scripts, oggetti "embedded", applets, etc.), e altre caratteristiche.

5.10.2 Autorizzazione

Ai 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.

5.10.3 Crittografia

Ai 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 OpenOffice: - L'utilizzo di firma digitale per la protezione dell'integrità dei documenti prodotti (attraverso l'azione "File → Digital Signatures"); - L'utilizzo di meccanismi per la protezione della confidenzialità dei documenti prodotti eseguendone la cifratura (attraverso l'azione "Save With Password").

5.10.4 Procedure

Ai 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	Dalla versione 2.1, OpenOffice ha incluso una funzionalità che segnala se è disponibile una nuova versione. Per attivare questa opzione: *Tools → Options → Online Update → Check for updates automatically* È possibile ricevere alerts via email su vulnerabilità di sicurezza risolte (vedi references: [1]); È possibile ricevere informazioni complete sugli alert per tutte le vulnerabilità di sicurezza risolte (vedi references: [2]). Tutte le patch di sicurezza devono essere installate prontamente.
References	[1] Security Alerts, https://www.openoffice.org/security/alerts.html [2] Security Bulletin, https://www.openoffice.org/security/bulletin.html

Limitare e controllare l'uso di open source "spurio"	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Poiché l'open source rende il codice sorgente disponibile a chiunque, un attaccante potrebbe: - progettare e distribuire alcuni malware incorporando codice dannoso nella distribuzione originale open source (al fine di lasciare backdoor o eseguire l'upload di dati sensibili o informazioni aziendali) - mostrare alcune caratteristiche interessanti della distribuzione malevola attirando così alcuni utenti finali. L'organizzazione deve definire una chiara politica di sicurezza sull'utilizzo di open source, per evitare che vengano scaricate e installate customizzazioni di software open source da fonti non attendibili, considerando le seguenti linee guida: - utilizzo di procedure di identificazione, autenticazione e autorizzazione per il software open source; - limitazione della disponibilità e tracciamento di tutti gli utilizzi di software open source; - rimozione o disabilitazione di tutti i programmi open source non necessari e non ammessi.

Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Assicurarsi che la copia di OpenOffice sia genuina: - scaricata da un sito attendibile (https://www.openoffice.org/download/); - acquisita da uno distributore ufficiale. Verificare il checksum per assicurarsi che la copia non sia stata danneggiata prima di installarla.

Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Falsificazione di identità. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Una macro può essere collegata a qualsiasi file OpenOffice (documento, foglio di lavoro, ecc.). Ogni volta che OpenOffice rileva le macro in un documento aperto, gestirà/eseguirà la macro come impostato a livello di "Security options → Macro security", che offre una protezione limitata. La regola più sicura è di non aprire alcun file OpenOffice a meno che non si abbia sicurezza della provenienza e fiducia del mittente, tanto più se contiene delle macro. Pertanto, se è necessario scambiare regolarmente documenti con soggetti ben individuati, si consiglia l'uso di firme digitali per certificare l'autenticità e l'integrità del documento.

Minaccia	Divulgazione di informazioni riservate.
Contromisure	Definire la modalità di segnalazione di eventuali vulnerabilità sospette o errori di OpenOffice al team di Sicurezza dell'organizzazione o dell'eventuale provider (in caso di servizi di sicurezza gestita) o a fornitori che erogano servizi di supporto tecnico, al fine di impedire la divulgazione di informazioni riservate. Occorre definire: - Quali informazioni si possono fornire. - Gli accordi di riservatezza.