Contromisure	- Attivare la “Relaying Protection” in modo che solo gli utenti identificati ed autorizzati possano collegarsi per l’invio di email. Disabilitare il funzionamento come "open relay". - Configurare inoltre il server in modo da accettare (in ingresso) o effettuare il relay (in uscita) solo per le email rispetto alle quali è autoritativo (per il dominio) e solo da e per caselle di posta effettivamente esistenti all’interno dell’organizzazione. - Infine quando il server è un relay host (il cui compito è di inoltrare i messaggi ad un altro SMTP server), utilizzare sempre l’autenticazione per la connessione tra i diversi server SMTP dell’architettura, utilizzando su ogni host il TLS 1.2 o successivo.

5.7.5 Crittografia

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

Protezione delle informazioni strumentali all'accesso	
Minaccia	- Attacchi all’integrità delle informazioni. - Compromissione delle comunicazioni. - Divulgazione di informazioni riservate. - Falsificazione di identità.
Contromisure	A livello di client mail, si tengano presenti: - L’utilizzo di meccanismi per la protezione dell'integrità e dell’autenticità delle informazioni trasmesse e/o ricevute via e-mail che prevedano utilizzo di strumenti crittografici, quali ad esempio la firma digitale. - L’utilizzo di meccanismi per la protezione della confidenzialità delle informazioni trasmesse e/o ricevute via e-mail eseguendo la cifratura dei messaggi end-to-end (cioè a livello dei client), con strumenti idonei ammessi dalla politica aziendale.

5.7.6 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.7.7 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].

5.7.8 Anti-Phishing

Software anti-phishing	
Minaccia	- Attacchi all’integrità dei sistemi. - Furto di credenziali di autenticazione. - Negazione dei servizi.
Contromisure	Mail Server: Installare sul Mail Server un modulo aggiuntivo anti-phishing che aggiorni il proprio database delle “firme” (pattern riconosciuti come pericolosi) almeno una volta al giorno. Mail Client: Prevedere per i client di posta aziendali, come Microsoft Outlook, un modulo aggiuntivo con il quale possano essere rilevati i collegamenti sospetti di un e-mail. Webmail: Utilizzare un browser recente e aggiornato, dotato di funzionalità di filtro