

<b>Contromisure</b>	<ul style="list-style-type: none"> <li>- 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".</li> <li>- 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.</li> <li>- 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.</li> </ul>
---------------------	--

### 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	
<b>Minaccia</b>	<ul style="list-style-type: none"> <li>- Attacchi all’integrità delle informazioni.</li> <li>- Compromissione delle comunicazioni.</li> <li>- Divulgazione di informazioni riservate.</li> <li>- Falsificazione di identità.</li> </ul>
<b>Contromisure</b>	<p>A livello di <u>client mail</u>, si tengano presenti:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul>

### 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	
<b>Minaccia</b>	<ul style="list-style-type: none"> <li>- Attacchi all’integrità dei sistemi.</li> <li>- Furto di credenziali di autenticazione.</li> <li>- Negazione dei servizi.</li> </ul>
<b>Contromisure</b>	<p><u>Mail Server</u>: 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.</p> <p><u>Mail Client</u>: 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.</p> <p><u>Webmail</u>: Utilizzare un browser recente e aggiornato, dotato di funzionalità di filtro</p>