Sezione: Sicurezza Informatica

Campo	Valore
Piattaforma	GDPRLab
Sezione	Sicurezza informatica
Destinatari	Consulenti tecnici / DPO / Rivenditori
Versione guida	1.0

1

1. Cos'è la sezione Sicurezza Informatica

La sezione Sicurezza Informatica raccoglie le informazioni sulle misure di protezione digitale adottate dall'organizzazione: protezioni perimetrali di rete, funzioni di sicurezza attive, segmentazione della rete, modalità di gestione e controllo, logging degli eventi e piani di backup.

Questi dati concorrono al calcolo del Compliance Score e documentano le misure tecniche ex art. 32 GDPR.

La sezione è a pagina unica con salvataggio esplicito tramite il pulsante Salva in alto a destra.

Si accede cliccando su **Sicurezza informatica** nel menu laterale sinistro.

2

2. KPI in evidenza (riga superiore)

In cima alla pagina sono presenti quattro card riepilogative che mostrano lo stato attuale delle principali aree di sicurezza:

Card	Colore	Stato iniziale	Significato
Firewall	Viola	No	Indica se è presente e configurato un firewall aziendale
Piani backup	Arancione	0	Numero di piani di backup configurati
Protezione rete	Verde	Non config.	Stato della configurazione della protezione perimetrale di rete
Logging	Rosso/ Rosa	Nessuna	Livello di registrazione degli eventi di sicurezza configurato

> ***Nota operativa:*** *I colori delle card riflettono il livello di configurazione: uno stato "No", "0" o "Non config." indica che quella misura non è ancora stata impostata. Compilare tutte le sezioni per far avanzare i KPI verso valori positivi.*

3

3. Protezioni perimetrali di rete

Il primo blocco della pagina riguarda le misure che proteggono l'intera azienda dall'accesso da internet.

Si seleziona il tipo di protezione perimetrale presente scegliendo una sola opzione tra le seguenti (radio button):

Opzione	Descrizione
Solo modem dell'operatore (nessun firewall dedicato)	La rete è protetta solo dal router fornito dal provider internet
Router configurato dal tecnico	Router aziendale con alcune regole di sicurezza impostate manualmente
Firewall aziendale dedicato	Apparato di sicurezza specifico installato per proteggere la rete
Firewall evoluto / UTM gestito	Firewall con funzioni avanzate e controlli periodici da parte del tecnico
Altro	Soluzione non classificabile nelle categorie precedenti

> ***Nota operativa:*** *La selezione di questa opzione aggiorna la card Firewall in cima alla pagina. Scegliere l'opzione che rispecchia fedelmente la situazione reale del cliente: la scelta impatta direttamente sul punteggio di sicurezza e sulla documentazione art. 32.*

4

4. Funzioni di sicurezza attive

Sotto la selezione del tipo di firewall sono disponibili le funzioni di sicurezza aggiuntive, selezionabili tramite checkbox (selezione multipla).

Sono disposte in griglia a due colonne:

Funzione	Descrizione
Blocco accessi dall'esterno (default deny)	Da internet non è possibile entrare nei computer aziendali salvo autorizzazioni esplicite
IDS/IPS – prevenzione intrusioni	Il sistema rileva e blocca tentativi di attacco informatico
Web/DNS filtering	Blocca automaticamente siti pericolosi o malevoli
Controllo applicazioni	Limita programmi o traffico non autorizzato
Protezione malware di rete	Analizza i dati in ingresso per individuare virus prima che arrivino ai PC
Geoblocking	Blocca connessioni provenienti da paesi ritenuti a rischio
VPN accesso remoto protetto	I dipendenti accedono dall'esterno tramite collegamento sicuro e cifrato

A destra della griglia è presente un tachimetro “% sicurezza” che si aggiorna in tempo reale al variare delle selezioni, con legenda cromatica:

→ Rosso: < 40% – livello insufficiente

→ Arancione: 40–60% – livello medio

→ Verde: ≥ 60% Buono – livello adeguato

5

5. Segmentazione rete

Questa sottosezione indica come è strutturata internamente la rete aziendale. Si seleziona una sola opzione (radio button):

Opzione	Significato
Rete unica per tutti	Tutti i dispositivi condividono la stessa rete senza separazioni
Rete uffici separata dalla Wi-Fi ospiti	La rete aziendale è isolata dalla rete Wi-Fi destinata agli ospiti/ visitatori
Server separati dalla rete utenti	I server aziendali si trovano su un segmento di rete separato dagli utenti

> ***Nota operativa:*** *Una corretta segmentazione della rete riduce il rischio di propagazione di attacchi e migliora il punteggio di sicurezza. Selezionare l’opzione che corrisponde alla realtà infrastrutturale del cliente.*

6

6. Gestione e controllo

Indica le modalità con cui viene gestita e monitorata la sicurezza informatica nel tempo. Le opzioni visibili nella sezione comprendono:

→ Nessuna gestione dopo l’installazione

→ Intervento tecnico solo in caso di problemi

→ Controlli periodici del tecnico informatico

> ***Nota operativa:*** *Selezionare l’opzione che descrive accuratamente il livello di presidio tecnico effettivo. Una gestione attiva e periodica contribuisce positivamente al punteggio di sicurezza.*

7

7. Logging

Indica il livello di registrazione degli eventi di sicurezza. Le opzioni disponibili sono (radio button):

Opzione	Descrizione	Livello
Nessuna registrazione eventi	Non vengono registrati log di accesso o sicurezza	Insufficiente
Registrazione locale	I log vengono salvati localmente sui dispositivi	Minimo
Log conservati e verificati	I log sono conservati in modo strutturato e verificati periodicamente	Adeguato

> ***Nota operativa:*** *La disponibilità di log verificati è un requisito importante in caso di data breach: permette di ricostruire gli accessi e le operazioni effettuate. La card Logging in cima alla pagina si aggiorna in base alla selezione effettuata.*

8

8. Backup aziendale

La sezione Backup aziendale documenta i sistemi utilizzati per evitare la perdita o il blocco dei dati aziendali.

È separata dal blocco delle protezioni di rete e si gestisce tramite piani di backup individuali.

8.1 Vista elenco piani di backup

La pagina Piani Backup & Continuità (raggiungibile anche tramite il link Gestisci piani backup) mostra la lista di tutti i piani configurati con le colonne:

Colonna	Contenuto
Nome	Nome identificativo del piano di backup
Tipo	Tipologia di dati o sistema oggetto del backup
Frequenza	Con quale cadenza viene eseguito il backup
Retention (giorni)	Per quanti giorni vengono conservate le copie
Cifrato	Se il backup è protetto da cifratura (Sì/No)
Immutabile	Se il backup non può essere modificato o cancellato (protezione ransomware)
Ultimo Test	Data dell'ultimo test di ripristino effettuato
Azioni	Modifica o eliminazione del piano

8.2 Form "Nuovo piano di backup"

Cliccando su **+ Nuovo piano di backup** si apre una modale con tre sezioni:

Cosa viene salvato (checkbox multiple)

Opzione	Descrizione
Nessun backup strutturato	Non esiste un sistema organizzato di backup
Solo alcuni PC manualmente	Backup manuali su singoli computer, non sistematici
Dati condivisi aziendali	File server, cartelle condivise e documenti aziendali
Server/gestionale	Backup del server applicativo o del sistema gestionale
Posta elettronica aziendale	Backup delle caselle email aziendali
Database o software gestionali	Backup dei database e degli applicativi gestionali

Modalità di esecuzione (radio button – una sola opzione)

Opzione	Descrizione
Manuale occasionale	Il backup viene eseguito manualmente e senza cadenza fissa
Automatico giornaliero	Il sistema esegue il backup automaticamente ogni giorno
Automatico più volte al giorno	Il backup automatico avviene più volte nell'arco della giornata
Backup continuo/versioning	Ogni modifica viene salvata in tempo reale con storico delle versioni

> ***Nota operativa:*** *La sezione "Dove vengono salvati" è visibile scorrendo verso il basso nella modale: può includere opzioni su supporti locali, cloud, offsite. Compilarla prima di cliccare Salva piano.*

> **Attenzione: Il campo Nome del backup è obbligatorio. Usare nomi descrittivi che identifichino chiaramente cosa viene salvato (es. "Backup server gestionale", "Backup email Exchange"): facilita la gestione nel tempo e la verifica in caso di incidente.**

9

9. Salvataggio della sezione

A differenza di altre sezioni della piattaforma, la Sicurezza Informatica non si salva automaticamente.

È necessario cliccare il pulsante **Salva** in alto a destra nella pagina dopo aver completato tutte le configurazioni.

> **Attenzione: Non dimenticare di cliccare Salva dopo ogni modifica. Se si naviga verso un'altra sezione senza salvare, le modifiche andranno perse.**

10

10. Workflow consigliato

→ Selezionare il tipo di protezione perimetrale (firewall) corrispondente alla realtà del cliente
→ Spuntare tutte le funzioni di sicurezza attive effettivamente presenti
→ Indicare la segmentazione di rete reale
→ Selezionare la modalità di gestione e controllo appropriata
→ Configurare il livello di logging adottato
→ Aggiungere almeno un piano di backup tramite + Nuovo piano di backup
→ Cliccare **Salva** in alto a destra per confermare tutte le modifiche

> ***Nota operativa:*** *Una sezione Sicurezza Informatica completamente compilata è tra le più impattanti sul Compliance Score: incide sia sulla card Firewall che su quella Piani backup e Logging nella Dashboard.*

11

11. Relazioni con altre sezioni

Sezione	Come usa i dati Sicurezza Informatica
Dashboard	Le card Firewall, Piani backup, Protezione rete e Logging riflettono questa sezione
Trattamenti	Le misure di sicurezza informatica vengono citate nelle schede dei trattamenti
Registro Trattamenti	Le misure tecniche art. 32 vengono documentate anche nel registro
DPIA	La valutazione d'impatto considera le misure di sicurezza qui configurate
Asset Management	Gli asset IT beneficiano delle protezioni qui dichiarate