

CONTROLLI SISTEMA INFORMATICO

DESCRIZIONE REQUISITO	VALUTAZIONE	EVIDENZE OGGETTIVE E NOTE
Descrizione tecnica di rete dell'organizzazione		
C'è uno o più amministratori di sistema?		
Che sistemi operativi utilizzate?		
Avete un dominio?		
E' attivo un sistema di users e groups? Inche modo sono gestiti i groups?		
E' stato creato uno o più user per ogni soggetto incaricato?		
Quali criteri sono applicati per la composizione della password?		
Avete una procedura per la disattivazione di uno user o di un group?		
Se si ogni quanto la eseguite?		
Chi è a conoscenza delle password degli users?		
Se solo lo user ne è in possesso, che processo attivate in caso di assenze prolungate?		
Avete un sistema di autenticazione integrata?		
Sui software gestionali che user usate?		

DESCRIZIONE REQUISITO	VALUTAZIONE	EVIDENZE OGGETTIVE E NOTE
Il personale è stato formato sulla custodia della propria password?		
Il personale è stato formato per non lasciare accessibile lo strumento durante la loro assenza?		
Avete in uso un software o uno strumento per il management delle password come policy aziendale?		
Vengono utilizzati strumenti come google drive, dropbox, wetranfert o similari?		
Se si con che utenti e per che scopi?		
Utilizzate servizi in cloud se si quali?		
Utilizzate esternamente strumenti che si collegano alla rete interna? Come?		
Avete delle policy di gestione dei supporti rimovibili?		
Come provvedere al rilasciare delle patch di sicurezza?		
E' presente un'area server protetta?		
Che sistemi di prevenzione utilizzate?		
Avete antivirus e quale è gestito?		
C'è un firewall e con quali servizi?		
Riuscite a monitorare la rete?		
Avete un inventario degli asset (dispositivi, software) aggiornato? E' automatico?		

DESCRIZIONE REQUISITO	VALUTAZIONE	EVIDENZE OGGETTIVE E NOTE
Possedete un sistema di data governance per avere visibilità sui cambiamenti che avvengo? Avete avvisi automatici?		
Come è gestita la posta elettronica? Interna o esterna? Mail con nome o area?		
Qual è attuale procedura di Backup? Testate il restore?		
Avere un piano di Business continuity		
Utilizzate strumenti di cifratura e swiping?		
E' presente la wifi? E come è strutturata?		

CONTROLLI SITO INTERNET

DESCRIZIONE REQUISITO	VALUTAZIONE	EVIDENZE OGGETTIVE E NOTE
Il sito risiede su un server interno o da un provider? Quale?		
Dove risiede l'hosting del sito		
Da già delle garanzie sulla normativa vigente		
E' protetto da un certificato SSL		

DESCRIZIONE REQUISITO	VALUTAZIONE	EVIDENZE OGGETTIVE E NOTE
Come viene gerstito il backup		
Sono presenti autorizzazioni utente per gli accessi? Ogni utente ha un login differenziato?		
Il sito si basa su un CMS?		
Se sì questo è mantenuto aggiornato contro le vulnerabilità?		
Sono presenti componenti di terze parti?		
Se si vengono aggironate costantemente?		
E' presente uno o più form per la raccolta dei dati personali degli utenti		
E' stata redatta una corretta informativa privacy per la raccolta?		
E' stata redatta idonea Policy Privacy del sito		
Amministrazione trasparente D.lgs 33/2013		
Privacy e Trasparenza: Linee guida del Garante 14/05/2014		
E' presente idonea informativa relativa all'utilizzo di cookies		
Sono presenti le Note Legali		

DESCRIZIONE REQUISITO	VALUTAZIONE	EVIDENZE OGGETTIVE E NOTE
Con la gestione del sito vengono gestite anche le mail?		
Se si è stato nomintao un amministratore della posta?		
Si può accedere alla posta tramite webmail, POP3 o IMAP?		
Chi governa il camnbio password della casella?		
Le caselle sono personali o istituzionali?		
Sono gestiti anche profili social o altro?		
Chi raccoglie i dati e chi li gestisce è stato opportunamente formato?		