

Comune di Cinisello Balsamo
Via XXV Aprile, 4 20092
Cinisello Balsamo (MI)

COMPILAZIONE QUESTIONARIO

DOMANDA	RISPOSTA
Indica il codice relativo al settore che meglio si adatta alla tua attività.	Amministrazione Comunale Ente Statale Locale
Riguardo pagamenti con carte di credito e carte di pagamento, seleziona l'opzione corretta :	I pagamenti sono accettati solo tramite canali online completamente esternalizzati tramite il circuito PAGO PA. Nessun dato delle carte di pagamento viene memorizzato, elaborato o trasmesso dal Comune.
Indica il numero dei dipendenti in forza alla tua attività	400
Indica il numero di dipendenti in forza alla tua attività specificatamente dedicati alla gestione del Sistema Informatico (da qui in avanti, Sistema IT)	14

Indica il numero di dipendenti in forza alla tua attività specificatamente dedicati alla gestione della Sicurezza del Sistema IT	3
Indica il numero (stimato) di server presenti nella tua azienda; per server ospitati in cloud, inserire il numero stimato di istanze.	100
Indica il numero (stimato) di workstation PC (Laptop/Desktop) presenti nella tua azienda.	500
Indica il numero (stimato) di soggetti i cui dati personali sono mantenuti all'interno della tua azienda.	75000 abitanti
Indica il budget annuale stanziato per la gestione e l'aggiornamento del Sistema IT aziendale (€)	600000
Indica il budget annuale stanziato per la sicurezza del Sistema IT aziendale (€)	75000
Indica, tra i seguenti, gli eventi che hanno interessato la tua azienda negli ultimi tre anni	nessuno
Indica gli eventuali Social Network sui quali la tua	Facebook

attività ha un profilo	Instagram Altro
La tua attività dispone di un responsabile della sicurezza IT con riporto diretto alla Direzione Aziendale (i.e. CISO - Chief Information Security Officer)	Sì
Indica se l'accesso al Sistema IT viene regolamentato e periodicamente aggiornato sulla base delle effettive necessità di accesso di ogni singolo utente per lo svolgimento della propria mansione (revisione periodica dei ruoli e dei privilegi assegnati)	Sì
Indica se l'accesso locale come Amministratore/Super User per le workstation viene generalmente inibito agli utenti, ad eccezione di casi tracciati e necessari per lo svolgimento delle mansioni tecniche di gestione dei sistemi IT	Sì
Sono definiti requisiti minimi per la forma e la durata delle password utente?	Sì
Indica come viene protetto l'eventuale accesso remoto ai sistemi/reti aziendali interni	L'accesso avviene con VPN o equivalente, con autenticazione a due fattori (MFA)
E' fisicamente prevista una zona ad accesso limitato dedicata al contenimento degli apparati e degli archivi contenenti dati strategici/critici per l'attività aziendale?	Sì
Sono previste procedure per la distruzione o il riutilizzo sicuro degli apparati dismessi?	Sì
E' definito ed implementato un processo o una attività di IT Risk Assessment?	Sì
E' previsto un elenco/inventario di tutti gli asset aziendali relativi al Sistema IT (software e hardware)?	Sì, operato automaticamente
Gli eventuali fornitori vengono preventivamente sottoposti ad una procedura di Valutazione del Rischio?	Sì Tutti i fornitori sono certificati ACN

Come vengono gestiti i backup?	Sono implementati strumenti di backup automatici
Quale è la periodicità dei backup per le informazioni critiche o strategiche?	Quotidiana
Con quale periodicità vengono installati gli aggiornamenti ("patch") di sicurezza?	Mensile o su segnalazione di vulnerabilità note
Quali contromisure sono adottate per la prevenzione delle minacce più rilevanti?	Firewall dedicato Autenticazione a due fattori (MFA) per l'accesso remoto ai servizi aziendali Segmentazione della rete / DMZ Soluzione dedicata di Email filtering (antispam, antivirus) EDR e EDP su tutte le postazioni
La tua attività sviluppa internamente applicazioni software strategiche per il business o critiche per l'operatività aziendale?	Sì
Sono svolte attività periodiche di formazione sulla sicurezza informatica e sulle politiche aziendali di sicurezza per il personale?	Sì, con cadenza annuale
Sono previste simulazioni periodiche di attacchi di phishing (i.e. esercitazioni di "white phishing") allo scopo di valutare la maturità del personale su questa tematica e la loro capacità di individuare attacchi di tipo Social Engineering?	Sì