Bozza questionario polizza cyber

Informazioni generali

Proponente
Denominazione: Provincia di Reggio Emilia
Indirizzo: Corso Garibaldi, 59 Reggio Emilia RE

Tipologia di Società Assicurato: Ente pubblico

Personale provinciale (dipendenti, personale distaccato e personale a contratto): circa 260 al 01/03/2018
Personale regionale operante su rete e dotazione informatica provinciale: circa 40 al 01/03/2018

Informazioni su asset e sistemi IT sulla rete aziendale

N. Users: circa 300
N. Desktops: circa 350
N. Laptops/Tablets: circa 100
N. Servers: circa 70 (fisici e virtuali)

Quantità totale indicativa di dati - data storage (espressa in gigabyte) 8000 Gb

Altri enti esterni a cui sono erogati servizi quali:

servizi applicativi (sistemi cartografici, raccolta di segnalazioni di degrado, gestione delle pratiche di sportello unico, gestione e pubblicazione dei dati elettorali, raccolta dati per il catalogo delle biblioteche provinciali, etc)	Circa 40 comuni
Servizi infrastrutturali (firewall per la rete interna e le pubblicazioni su internet, firewall IPS (Intrusion Prevent System) per la navigazione internet, protezione del servizio di posta elettronica mediante il servizio di relay provinciale, indirizzamenti IP, dns	Circa 25 comuni

E' stata stipulato un accordo con gli Enti per la gestione di questi servizi?
SI

Procedure di Protezione e training

- Esiste un documento scritto, approvato e formalizzato, sui Sistemi di Sicurezza delle Informazioni (ISS)?
  SI
- Tale documento è stato approvato dai responsabili e comunicato a tutto il personale?
  Non viene diffuso per motivi di sicurezza
- E' stata fornita a tutti i dipendenti una copia delle procedure per il trattamento e la protezione dei dati adottate dall'Ente, che sono tenuti a rispettare e alle quali debbano aderire?
  Una sintesi è contenuta nel documento di nomina ad incaricato
- L'Ente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali?
  SI
- L'Ente fornisce corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici?
  SI

Controlli dei sistemi informatici – Sicurezza della rete

- Avete un programma attivo di protezione dai virus su tutte le workstation, i server e i "mission critical server" per proteggersi contro virus, worms, spyware e/o altro malware?
  SI
- Avete una procedura attiva per il controllo e l'aggiornamento del software, incluse patches e aggiornamenti dell'anti-virus?
  SI
- Utilizzate firewall per prevenire l'accesso non autorizzato da reti e computer esterni alla rete aziendale con un Intrusion Detection System (IDS) attivo e regolarmente aggiornato?

SI

- Esistono regole di sicurezza e procedure per la gestione degli incidenti e delle variazioni relative alla gestione dei sistemi informativi, della loro configurazione e della loro operatività?
  SI
- Avete una procedura attiva per gestire gli account, incluso la rimozione degli account scaduti?
  SI
- Avete procedure di controllo accessi a sistemi informatici, alle proprie banche dati, ai centri di raccolta dati e a dati sensibili?
  SI
- Si dispone di un sistema di backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni?
  SI
- Il piano di backup è formalizzato e aggiornato periodicamente?
  SI
- Raccogliete, registrate, mantenete o distribuite carte di credito, altre carte di pagamento?
  NO
- Raccogliete, registrate, mantenete o distribuite altri dati che possano essere classificati come personali e sensibili?

Dati identificabili personali di terzi	SI
Informazioni sanitarie personali di terzi	SI
Informazioni relative a proprietà intellettuali	NO
Informazioni relative a transazioni monetarie e finanziarie	NO?
Informazioni relative a Dati Aziendali di Valore (o riservati)	SI

- Qualora sia stata selezionata almeno una delle voci sovrastanti, l'accesso ai dati sensibili è oggetto di restrizioni?
  SI
- Indicare chi ha accesso ai dati sensibili
  Amministratori di Sistema e Responsabili dei procedimenti che necessitano il trattamento dei dati, oltre che al personale incaricato.
- Utilizzate sistemi di crittografia dei dati, per proteggere l'integrità dei dati sensibili, inclusi i dati su apparecchiature elettroniche portatili (es. laptops, supporti di backup, DVD, dischi, memorie USB, ecc.)?
  NO
- E' stato implementato un sistema di monitoraggio proattivo contro le intrusioni?
  NO
- L'accesso a Internet degli utenti è limitato e controllato?
  SI, si accede soltanto dopo autenticazione
- Gli utenti possono accedere a:

social networks or blogs	SI
caselle email personali esterne	SI
instant messaging	SI

Protezione delle informazioni e Controllo degli accessi

- Esiste un inventario formale dei sistemi critici, delle applicazioni e della infrastruttura?
  SI
- Esiste una procedura di classificazione delle informazioni secondo il loro grado di sensibilità/criticità (integrità, riservatezza e disponibilità)?

SI

- L'accesso ai sistemi informativi richiede l'identificazione e l'autenticazione degli utenti interni e remoti con ID univoco?
  SI
- Gli utenti esterni devono essere autorizzati per accedere ai sistemi informativi della Ente?
  SI
- Esiste una procedura che impone il cambio periodico delle password e la loro complessità (strong password policy) per l'accesso ai sistemi informativi e ad operazioni critiche?
  SI
- I permessi di accesso sono differenziati in base al ruolo dell'utente in accordo con il principio del least/minimal privilege?
  SI
- Esiste una procedura di gestione e controllo delle autorizzazioni, che comprende revisioni periodiche dei permessi?
  SI
- Gli utenti hanno accesso ai sistemi con l'utilizzo di strumenti personali (es. telefono, tablet)?
  NO
- La gestione dei computer è centralizzata?
  SI
- Gli utenti sono amministratori delle loro workstation?
  NO
- I laptop sono protetti dal personal firewall?
  NO
- I laptop possono connettersi a Internet solo via rete interna?
  NO

Fornitori e terze parti

- Si esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete?
  NO
- secondo quale modalità vengono gestiti i data center?
  In house e in parte esternalizzati in cloud non di privati (Lepida SPA società in house della regione ER e dell'Ente)
- Si esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?
  SI
- SI richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi?
  SI
- E' permesso ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT?
  Si ma soltanto previa autorizzazione e l'utilizzo degli standard aziendali

Contenuti multimediali, website e social network

- Esistono procedure per verificare che il contenuto delle pagine internet (a cui gli utenti accedono) non infranga i diritti di proprietà intellettuale?
  NO, soltanto prassi di controllo
- Esistono procedure per verificare che il contenuto delle pagine internet (a cui gli utenti accedono) non porti a danni personali che includono diffamazione e calunnia?
  NO, soltanto prassi di controllo
- I vostri website includono (o includeranno) chatrooms, blogs o message boards o altro che permettono agli utenti di fare upload o scambiare messaggi?
  NO
- I vostri website includono (o includeranno) servizi di networking per terze parti tra cui social networking o blogs ?
  NO

Sinistri e circostanze

- E' a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o

controllo, o da parte di chiunque se ne occupi per conto dell'Ente nei tre anni precedenti a questa richiesta?
NO

- Ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta?
  NO
- La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta?
  L'Ente da assicurare, ha mai dovuto effettuare una comunicazione ai propri clienti o a soggetti terzi (data subject) a seguito di una violazione di loro dati.
  NO
- L'Ente da assicurare, è mai stata oggetto di un Avviso di Esecuzione da parte dell'Autorità Garante per la Protezione dei Dati Personali o altra Autorità regolamentatrice?
  NO

Sicurezza fisica

- I sistemi critici sono ubicati in almeno una sala macchine dedicata con un accesso ristretto e controllato?
  SI
- I sistemi critici sono ubicati in un Datacenter o in un luogo con un equivalente livello di sicurezza?
  In parte nei datacenter di Lepida spa
- La fornitura elettrica prevede UPS e batterie.
  SI
- UPS e batterie sono soggetti a regolare manutenzione?
  SI
- Esiste un generatore di corrente elettrica di back-up?
  NO