QUESTIONARIO POLIZZA CYBER

Informazioni generali

Proponente
Denominazione: Provincia di Reggio Emilia
Indirizzo: Corso Garibaldi, 54 42121 Reggio Emilia

Tipologia di Società Assicurato:

Personale (dipendenti, personale distaccato e personale a contratto): circa 210 al 19/04/2021
Personale esterno operante su rete e dotazione informatica: circa 40 al 19/04/2021

Informazioni su asset e sistemi IT sulla rete aziendale

N. Users: circa 220
N. Desktops: circa 300……..
N. Laptops/Tablets: circa 150……..
N. Servers: circa 70 (fisici e virtuali)……
ALTRO ……

Quantità totale indicativa di dati - data storage (espressa in gigabyte): 30000 Gb

Altri enti esterni a cui sono erogati servizi quali:

Servizi applicativi (sistemi cartografici, raccolta di segnalazioni di degrado, gestione delle pratiche, pubblicazione cataloghi speciali delle biblioteche, 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~~
- NO

Se **SI** con che Ente?
Tutte le Unioni della provincia in rappresentanza dei loro comuni ed il comune capoluogo

Procedure di Protezione e training

Esiste un documento scritto, approvato e formalizzato, sui Sistemi di Sicurezza delle Informazioni (ISS)?
- ~~SI~~
- NO

Tale documento è stato approvato dai responsabili e comunicato a tutto il personale?
Esistono diversi documenti approvati quali il DPS e i relativi allegati tecnici, le misure minime di sicurezza previste da Agid e il piano per la gestione degli incidenti. Sono pubblicate sulla intranet le informazioni generali ed organizzative, invece sono riservati gli allegati tecnici data la riservatezza dei dati.

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?
……...

L'Ente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali?
- ~~SI~~
- NO

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~~
- NO

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~~
- NO

Avete una procedura attiva per il controllo e l'aggiornamento del software, incluse patches e aggiornamenti dell'anti-virus?

- ~~SI~~
- NO

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~~
- NO

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~~
- NO

Avete una procedura attiva per gestire gli account, incluso la rimozione degli account scaduti?

- ~~SI~~
- NO

Avete procedure di controllo accessi a sistemi informatici, alle proprie banche dati, ai centri di raccolta dati e a dati sensibili?

- ~~SI~~
- NO

Si dispone di un sistema di backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni?

- ~~SI~~
- NO

Il piano di backup è formalizzato e aggiornato periodicamente?

- ~~SI~~
- NO

Raccogliete, registrate, mantenete o distribuite carte di credito, altre carte di pagamento?

- SI
- ~~NO~~

Raccogliete, registrate, mantenete o distribuite altri dati che possano essere classificati come personali e sensibili?

Dati identificabili personali di terzi	~~SI~~ NO
Informazioni sanitarie personali di terzi	~~SI~~ NO
Informazioni relative a proprietà intellettuali	SI ~~NO~~
Informazioni relative a transazioni monetarie e finanziarie	~~SI~~ NO
Informazioni relative a Dati Aziendali di	~~SI~~

Valore (o riservati)	○ NO

Qualora sia stata selezionata almeno una delle voci sovrastanti, l'accesso ai dati sensibili è oggetto di restrizioni?

- ~~○ SI~~
- ○ NO

Indicare chi ha accesso ai dati sensibili
Tutte le procedure e i dati sono profilati secondo la necessità di operare sugli stessi, prevalentemente a seconda del Servizio/unità Operativa di appartenenza

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.)?

- ~~○ SI~~
- ○ NO

E' stato implementato un sistema di monitoraggio proattivo contro le intrusioni?

- ~~○ SI~~
- ○ NO

L'accesso a Internet degli utenti è limitato e controllato?

- ~~○ SI~~
- ○ NO

Gli utenti possono accedere a:

Social networks or blogs	~~○ SI~~ ○ NO
Caselle email personali esterne	~~○ SI~~ ○ NO
Instant messaging	~~○ SI~~ ○ NO

Protezione delle informazioni e Controllo degli accessi

Esiste un inventario formale dei sistemi critici, delle applicazioni e della infrastruttura?

- ~~○ SI~~
- ○ NO

Esiste una procedura di classificazione delle informazioni secondo il loro grado di sensibilità/criticità (integrità, riservatezza e disponibilità)?

- ~~○ SI registro dei trattamenti?~~
- ○ NO

L'accesso ai sistemi informativi richiede l'identificazione e l'autenticazione degli utenti interni e remoti con ID univoco?

- ~~○ SI~~
- ○ NO

Gli utenti esterni devono essere autorizzati per accedere ai sistemi informativi della Ente?

- ~~○ SI~~
- ○ NO

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~~
- NO

I permessi di accesso sono differenziati in base al ruolo dell'utente in accordo con il principio del least/minimal privilege?

- ~~SI~~
- NO

Esiste una procedura di gestione e controllo delle autorizzazioni, che comprende revisioni periodiche dei permessi?

- ~~SI~~
- NO

Gli utenti hanno accesso ai sistemi con l'utilizzo di strumenti personali (es. telefono, tablet)?

- ~~SI solo posta elettronica~~
- NO

La gestione dei computer è centralizzata?

- ~~SI~~
- NO

Gli utenti sono amministratori delle loro workstation?

- SI
- ~~NO~~

I laptop sono protetti dal personal firewall?

- ~~SI~~
- NO

I laptop possono connettersi a Internet solo via rete interna?

- SI
- ~~NO~~

Fornitori e terze parti

Si esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete?

- ~~SI~~
- NO

Secondo quale modalità vengono gestiti i data center?

Parte dei server sono ancora presso la sala macchine dell'Ente e sono in completa gestione al personale interno. Sono poi stati spostati alcuni servizi presso un datacenter di Lepida (società partecipata) su cui la gestione sistemistica di base è effettuata dal personale di Lepida, il resto da personale interno all'Ente. Nel corso del prossimo biennio tutti i server in produzione verranno migrati presso il datacenter di Lepida e il personale interno ne sarà amministratore.

Si esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

- ~~SI~~
- NO

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~~
- NO

E' permesso ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT?

- ~~SI~~
- NO

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?

- SI
- ~~NO~~

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?

- ~~SI~~
- NO

I vostri website includono (o includeranno) chatrooms, blogs o message boards o altro che permettono agli utenti di fare upload o scambiare messaggi?

- SI
- ~~NO~~

I vostri website includono (o includeranno) servizi di networking per terze parti tra cui social networking o blogs ?

- SI
- ~~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?

- SI
- ~~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?

- SI
- ~~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?

- SI
- ~~NO~~

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?

- SI
- ~~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?

- SI
- ~~NO~~

Sicurezza fisica

I sistemi critici sono ubicati in almeno una sala macchine dedicata con un accesso ristretto e controllato?

- ~~SI~~
- NO

I sistemi critici sono ubicati in un Datacenter o in un luogo con un equivalente livello di sicurezza?
Come indicato nelle domande precedenti, parte dei server sono ancora presso la sala macchine dell'Ente e

alcuni servizi presso un datacenter di Lepida e nel corso del prossimo biennio tutti i server in produzione verranno migrati presso il datacenter di Lepida.
……

La fornitura elettrica prevede UPS e batterie?

- ~~SI~~
- NO

UPS e batterie sono soggetti a regolare manutenzione?

- ~~SI~~
- NO

Esiste un generatore di corrente elettrica di back-up?

- SI
- ~~NO~~