Politica per la sicurezza delle informazioni

L'organizzazione fornisce indicazioni e supporto da parte della Direzione per la sicurezza delle informazioni nel rispetto dei requisiti aziendali e della legislazione vigente.

Documento relativo alla politica per la sicurezza delle informazioni

La Direzione della SoES spa, nell'ambito di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, che comprende il trattamento e i dati inerenti a: *Gestione di aree di sosta a pagamento, gestione e rendicontazione di sanzioni amministrative per infrazioni al codice della strada commesse da cittadini residenti in Italia e all'estero. Gestione e trattamento dei relativi dati mediante strumenti informatici. Noleggio hardware e software per il rilevamento delle infrazioni al Codice della strada. Sviluppo di applicativi software. Servizi afferenti la gestione della riscossione volontaria e coattiva dei crediti della P.A. Servizi di supporto afferenti la gestione del contenzioso legale nei procedimenti Amministrativi della P.A.* svolti presso l'unità operativa di Minturno, alla via Antonio Sebastiani, 77, si impegna a garantire la riservatezza, l'integrità e la disponibilità di tutte le risorse, sia fisiche sia elettroniche, al fine di preservare il proprio livello di competitività e di redditività e la propria immagine commerciale, nel rispetto di leggi, regolamenti e obblighi contrattuali. I requisiti di sicurezza delle informazioni e il relativo Sistema sono e continueranno ad essere lo strumento per l'utilizzo e la condivisione delle informazioni in condizioni di rischio ridotte a livelli accettabili.

L'attuale strategia di crescita aziendale, inquadrata in un contesto di gestione del rischio, crea la situazione per identificare, verificare, valutare e controllare i rischi legati al trattamento delle informazioni mediante l'istituzione e la gestione di un ISMS. La valutazione dei rischi, la dichiarazione di applicabilità e il piano di trattamento dei rischi sono gli opportuni strumenti per definire come i suddetti rischi sono tenuti sotto controllo.

La non interrompibilità delle attività aziendali (business continuity), i piani di emergenza, le procedure per il back up dei dati, la prevenzione contro i virus informatici e le attività degli hacker, il controllo degli accessi ai sistemi e la registrazione di eventuali problemi di sicurezza sono tra i princìpi alla base di questa Politica. Il Manuale dell'ISMS prevede obiettivi di controllo per ciascuno di questi punti, supportati da ulteriori politiche e procedure.

Ciascun dipendente dell'Organizzazione è tenuto al rispetto di questa Politica e di quanto stabilito dal Sistema di Gestione della Sicurezza Informatica, così come lo sono gli eventuali operatori appartenenti a terze parti fornitrici di servizi all'Azienda. Allo scopo, è gestita l'apposita formazione.

L'ISMS è soggetto a continue e sistematiche revisioni e miglioramenti: alla luce di ciò la Direzione ha delegato nello specifico al responsabile dell'ISMS, supportato dai responsabili d'area, amministratori di sistema e consulenti esterni, il ruolo della gestione del suddetto, nell'ambito del conseguimento e del mantenimento della certificazione secondo la Norma ISO 27001:2013.

Di seguito si riportano gli obiettivi di sicurezza perseguiti dall'organizzazione:

- Adeguato numero di ore/incontri di formazione e sensibilizzazione effettuati agli operatori coinvolti nel trattamento delle informazioni;
- Completezza dell'invetario degli asset;
- Raggiungimento della politica del Need to know, per esempio mediante adeguata profilazione degli utenti;
- Monitoraggio dei fornitori di servizi esterni;
- Controllo degli accessi e dei log dei sistemi;
- Completezza e chiarezza delle procedure operative;
- Efficienza ed efficacia delle contromisure di accesso fisico;
- Protezione contro attacchi di CyberSecurity;
- Gestione dei cambiamenti;
- Gestione delle vulnerabilità tecniche e degli incidenti di sicurezza;
- Gestione della continuità operativa;
- Gestione della compliance

Nel corso dei review meeting vengono definite le metriche per misurare il grado di raggiungimenti degli obiettivi.

Servizi erogati in modalità cloud

Soes eroga servizi di cloud computing in modalità SaaS (Cloud Service Provider), Software-as-a-Service) in quanto i servizi all'utente finale sono erogati tramite applicazioni basate sul Web. Il modello SaaS è un metodo per la distribuzione di applicazioni software tramite Internet, dove i provider di servizi cloud ospitano e gestiscono tali applicazioni software per consentire l'uso della stessa applicazione da tutti i tuoi dispositivi accedendovi nel cloud.

Soes nell'utilizzare la infrastruttura IAAS a supporto dei propri processi acquisisce il ruolo di Cloud Service Customer.

La segregazione dei vari tenant (End User) è garantita tramite l'utilizzo di container Docker. Docker è un progetto open-source che automatizza il deployment di applicazioni all'interno di contenitori software, fornendo un'astrazione aggiuntiva grazie alla virtualizzazione a livello di sistema operativo di Linux.

<u>Cloud service provider</u>

Il Cloud Soes offre all'utente finale i seguenti servizi a valore aggiunto:

- Piattaforma di CRM per richiedere modifiche al servizio
- Piattaforma di autenticazione centralizzata (single sign on)

La segregazione della parte amministrativa del fornitore e del cliente è garantita dalla tipologia di servizio erogato che limita gli accessi dell'end user alla sola piattaforma SGV e non alla sottostante piattaforma IAAS.

In ambito Accesss Control sono state implementate tecniche di single sign-on, ovvero un sistema di controllo d'accesso tale da consentire ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato. Gli obiettivi sono multipli:

- semplificare la gestione delle password: maggiore è il numero delle password da gestire, maggiore è la possibilità che vengano utilizzate password simili le une alle altre e facili da memorizzare, abbassando così il livello di sicurezza;
- semplificare la gestione degli accessi ai vari servizi;
- semplificare la definizione e la gestione delle politiche di sicurezza.

Si intravedono i seguenti rischi relativi da utenti autorizzati del servizio:

- Utilizzo da parte degli utenti finali tale da poter creare decadimento sulle performance dell'infrastruttura
- Accessi non necessari da parte di utenti autorizzati

Per la individuazione delle contromisure viene effettua apposita alla valutazione dei rischi.

L'accesso alle funzioni amministrative è disponibile anche la funzionalità di Two-Factor Authentication sia per accedere all'infrastruttura IAAS che SAAS.

Nell'ambito della gestione dei cambiamenti Soes comunica ai vari End User mediante email ogni attività di manutenzione e/o upgrade dei sistemi indicando eventuali disservizi previsti.

La sicurezza della virtualizzazione è garantita dalla infrastruttura IAAS che è basata sulla tecnologia Vmware vCloud Director che fornisce ambienti di rete separati logicamente e protetti da firewall per salvaguardare i requisiti di sicurezza aziendali e garantire protezione e isolamento adeguati.

La gestione ed il provvisioning degli account clienti, avviene tramite richiesta del referente dell'Ente al sistema di CRM disponibile su portale utente.

La comunicazione dei data breach avviene in conformità alle procedure aziendali PDP 10.1A - Procedura di DataBreach.

L'accesso agli asset del cliente avviene in relazione alle disposizioni contrattuali ed in conformità con le dispositivi legislative.

Cloud service customer

Soes utilizza un provider certificato CSP qualificato Tipo C.

Di seguito le policy utilizzate:

- Le informazioni storicizzate nell'ambiente cloud possono avere accesso al cloud service, fermo restante che per le macchine a livello di sistema operativo viene applicato la cifratura del dato.
- I processi girano in un multi-tenant virtualizzato cloud service mediante tecnologie Vmware Vcloud Director.
- Gli utenti amministrativi e non che accedono ai servizi sono solo quelli di Soes
- La locazione dei CED del cloud provider utilizzati è Italia.

Revisioni della politica per la sicurezza delle informazioni

La politica per la sicurezza delle informazioni è revisionata annualmente o quando intervenga un evento significativo che ne comporti l'aggiornamento, per assicurarne l'idoneità, l'adeguatezza e l'efficacia.

Il responsabile dell'ISMS è l'affidatario del documento e ne ha la responsabilità per l'aggiornamento, la revisione e la valutazione. Le modifiche alla politica devono essere approvate dalla Direzione.

DATA
11/01/2021

RSG