Velocar

Speed and traffic detection technologies

Velocar
Politica per la sicurezza delle informazioni
Politica nell'uso delle reti virtuali

INDICE

Rev.	Data	Redazione	Verifica - Approvazione (DG)	Note
00	09/04/16	Raffaele Annunziata ENGINEERING & CONSULTING	PAOLO BAZZOLI	*1ª EMISSIONE*
01	16/08/19	Raffaele Annunziata ENGINEERING & CONSULTING	PAOLO BAZZOLI	*Estensione ISO 27017 ISO 27018*

1 SCOPO

La direzione di VELOCAR S.R.L. ha definito, divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente "*politica"* per la Gestione della Sicurezza delle Informazioni, nonché quella relativa al proprio *"cloud computing"*

Lo scopo della presente policy è di garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nonché ai requisiti previsti dalle norme ISO/IEC 27017 e 27018 nell'ambito del *cloud computing*.

L'applicazione della Gestione della Sicurezza delle informazioni per l'organizzazione si riferisce a tutte le attività che riguardano i dati provenienti dalle rilevazioni (fotogrammi e video) registrate dalle apparecchiature stradali installate, nonché dei relativi software gestionali rilasciati in uso ai clienti per l'accesso e ed il trattamento di tali dati.

2 CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutte le parti interessate, interne ed. sterne all'organizzazione. L'attuazione della presente politica è obbligatoria a tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni, l'uso del software di gestione, nonché il servizio di *"cloud computing"* del tipo SaaS, rientranti nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), ovvero per tutti i dati provenienti dalle apparecchiature per il controllo del traffico stradale.

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti, nonché delle regole e dei livelli di sicurezza imposti dalla direzione aziendale, nell'ambito della riduzione dei rischi.

3 POLICY

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti.

L'organizzazione si pone come obbiettivi primari quello di assicurare:

la riservatezza delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato;

l'integrità delle informazioni: ovvero proteggere la precisione e la completezza;

delle informazioni e dei metodi per la loro elaborazione.

la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La Velocar è cosciente che la mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di sanzioni legate alla violazione delle vigenti normative in materia di protezione dei dati, nonché danni di natura economica e finanziaria. Un adeguato livello di sicurezza deve essere esteso anche alle fasi di condivisione delle informazioni, qualora ve ne sia la necessità.

L'organizzazione identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema hardware e software. La valutazione del rischio permette di valutare a fronte della realistica probabilità di attuazione delle minacce identificate, le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza idonee.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati nonché per la scelta di implementare ulteriori misure di sicurezza.

La gestione della sicurezza delle informazioni prevede:

- il costante aggiornato degli asset aziendali rilevanti, ai fini della gestione delle informazioni e l'individuazione per ciascuno di un responsabile.
- la classificazione delle informazioni trattate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

Per garantire la sicurezza delle informazioni, sia interne sia quelle su piattaforma "*cloud"*, ovvero ogni accesso ai sistemi deve essere sottoposto a una procedura di identificazione e di autenticazione dell'utente. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita: isolamento cliente "*multi-tenancy e cloud service"*. Le modalità

di accesso devono essere periodicamente sottoposte a revisione da parte del gestore del sistema informatico.

Devono essere definite delle procedure per l'utilizzo sicuro degli asset e delle informazioni e de loro relativi sistemi di gestione hardware e software.

Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni a tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.

Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.

È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.

Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.

Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.

Gli aspetti di sicurezza delle informazioni compresi i sistemi di "*cloud computing"*, devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi hardware e software, delle apparecchiature installate e dei servizi "*cloud"* annessi.

Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

L'osservanza e l'attuazione di questa policy sono responsabilità di:

- Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni;
- Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda.
- Di tutti gli utilizzatori (clienti) che usufruiscono dei servizi di "*cloud"* messi a disposizione.

Il Responsabile della sicurezza delle informazioni, nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali;
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

3.1 Politica reti virtuali (VPN)

Per garantire la sicurezza delle informazioni raccolte dalle apparecchiature per il controllo stradale che vengono trasmesse o ai server di Velocar (cloud computing) o ai centri dati dei Comuni è impiegata una VPN (Virtual Private Network).

Nello specifico trattasi di una rete di telecomunicazioni privata tra soggetti che utilizzano un protocollo di trasmissione dati pubblico e condiviso (es. Internet).

- Per garantire la sicurezza delle informazioni sono impiegati tre differenti metodi:
- Credenziali di accesso della VPN (login e password).
- Crittografia dei dati.
- Blocco degli indirizzi IP non riconosciuti.
- Monitoraggio dei file di log.

Credenziali di accesso della VPN (login e password)

Il primo metodo di protezione dei dati è assicurarsi che chi li sta visualizzando sia davvero chi dice di essere, ed un modo per farlo è l'autenticazione tramite login e password che vengono definiti nel momento in cui viene installata l'apparecchiatura per il controllo stradale.

Crittografia dei dati

Le Secure VPN utilizzano protocolli crittografici a tunnel per offrire l'autenticazione del mittente e l'integrità del messaggio allo scopo di difendere la privacy.

Blocco degli indirizzi IP non riconosciuti

All'interno del firewall Velocar riporta quali sono gli indirizzi IP ai quali è consentito l'accesso.

Monitoraggio dei file di log

È possibile monitorare tutti gli eventi legati ad accessi autorizzati e non autorizzati ed eventuali operazioni di modifica del firewall.

4 RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business e delle condizioni legali.

Il Responsabile della sicurezza delle informazioni ha la responsabilità del riesame della politica della sicurezza delle informazioni.

Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica per la sicurezza delle informazioni. Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami. Particolare attenzione sarà prestata agli incidenti segnalati relativi alla sicurezza delle informazioni e alle tendenze relative alle minacce e vulnerabilità.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni, dei controlli e nell'allocazione delle risorse e delle responsabilità.

5 IMPEGNO DELLA DIREZIONE

La direzione sostiene attivamente la sicurezza dell'azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui obbiettivi principali sono:

- garantire che siano identificati tutti i requisiti che garantiscono la sicurezza delle informazioni e che questi incontrino le esigenze e le aspettative dei clienti;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- garantire il soddisfacimento di tutti i requisiti normativi e legislativi nazionali e comunitari in materia di trattamento dei dati personali con particolare riguardo ai dati sensibili;
- controllare che il SGSI sia integrato in tutti i processi aziendali
- attuare i tutti i controlli applicabili alle informazioni, ai sistemi ed alle procedure dell'organizzazione;
- monitorare i cambiamenti dell'esposizione alle minacce delle informazioni chiave dell'azienda, in fase di sviluppo e progettazione di nuove apparecchiature, software e sistemi di trattamento ed immagazzinamento dei dati.
- monitorare i cambiamenti tecnologici che consentono di migliorare la sicurezza delle informazioni;
- analizzare i data bridge, anche al fine di riesaminare i criteri di valutazione del rischio e i livelli di accettabilità degli stessi;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza;
- supportare i clienti che usufruiscono dei servizi aziendali nonché i clienti del servizio cloud a migliorare la propria gestione della sicurezza delle informazioni, nonché i rischi a cui sono esposte le informazioni inserite all'interno del servizio.
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni all'interno della propria organizzazione nonché alle parti esterne interessate.
- Analizzare attraverso dei test eseguiti da enti esterni al fine di verificare le eventuali vulnerabilità della rete o degli applicativi cloud utilizzati dai clienti.

- Utilizzare un sistema di criptografia dei file sempre aggiornato.

La presente politica adottata per il SGSI non dovrà essere in contrasto con quanto definito all'interno della mission aziendale avente come obbiettivo il rafforzamento dei rapporti con i clienti ed i fornitori nell'ottica del rispetto di quanto già applicato con le esistenti certificazioni ISO 9001 ed ISO 14001.