Sicurezza delle Informazioni: Il Nostro Impegno

Rif. ID 1.5 19/09/2024

Livello di classificazione: PUBBLICO

gsa
gestione servizi aziendali

Indice delle revisioni

Ed.	Rev.	Data	Descrizione
1	0	19.09.24	Emissione documento

SOMMARIO

Premessa

La direzione di GSA nell'ambito dei propri processi prevede l'implementazione e l'attuazione di misure organizzative, tecniche e procedurali per proteggere e salvaguardare le informazioni.
Il patrimonio informativo è un asset fondamentale per GSA. L'eterogeneità dei servizi offerti, il numero e la tipologia di clienti impone una corretta attenzione verso la salvaguardia delle informazioni. La base informativa è costantemente arricchita dal "business ricorrente" e da nuove opportunità che GSA sta perseguendo in termini di business digitale per rendere più efficace la propria offerta e differenziare le proprie attività all'interno del gruppo.
In particolare, le informazioni devono essere mantenute integre, disponibili ed accessibili solo a chi ha la corretta autorizzazione.

La direzione ha quindi definito i seguenti macro-obiettivi per la sicurezza delle informazioni:

- l'immagine dell'azienda, quale fornitore affidabile e competente, deve essere garantita con tutti i mezzi possibili ed al meglio delle possibilità;
- l'operato dell'azienda deve rispondere pienamente alle indicazioni delle normative vigenti e cogenti (es. Regolamento Ue 2016/679);
- GSA deve essere in grado di rispondere pienamente ai requisiti contrattuali, impliciti ed espliciti, sottoscritti con i propri clienti, in particolare per l'erogazione dei nuovi servizi digitali offerti;
- GSA deve adottare misure per fidelizzare, professionalizzare e per aumentare il livello di sensibilità del personale.

Per raggiungere gli obiettivi appena elencati GSA si impegna a:

- promuovere sistematicamente la formazione del personale con particolare riferimento ai temi inerenti alla sicurezza dell'informazione e al rischio aziendale (incluso quello legato al soddisfacimento delle norme);
- aggiornare e comunicare internamente un organigramma aziendale che preveda esplicitamente figure preposte alla "Gestione per la Sicurezza" inclusa la gestione del Sistema di Gestione per la Sicurezza delle informazioni (SGSI);
- promuovere, presidiare e mantenere processi di crescita e di ricerca di miglioramento continuo.
-

Nel seguito del documento sono definiti obiettivi di dettaglio (identificabili nel documento dal simbolo ).
Le modalità di attuazione di ogni obiettivo sono definite all'interno dei documenti del SGSI.

Organizzazione per la sicurezza delle informazioni

Organizzazione interna

Stabilire un riferimento organizzativo per sviluppare e monitorare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'azienda.

Devono essere definite ed assegnate le responsabilità inerenti alla sicurezza delle informazioni.

Dispositivi portatili

Garantire una gestione sicura nell'utilizzo dei dispositivi portatili.

Risorse umane

Prima dell'impiego

Garantire che il personale e i collaboratori siano adeguati al ruolo e ne comprendano le responsabilità.

Devono essere svolti controlli per la verifica su tutti i candidati all'impiego, in accordo con le leggi e regolamenti. In particolare, l'azienda si deve accertare che il candidato abbia le necessarie competenze per svolgere il proprio ruolo nel rispetto della sicurezza delle informazioni.

Durante l'impiego

Garantire che il personale sia a conoscenza delle responsabilità per la sicurezza delle informazioni ed adempia correttamente alle relative mansioni.

Deve essere erogata a tutto il personale un'adeguata formazione sulle politiche e procedure organizzative in merito alla sicurezza delle informazioni.

Cessazione e variazione del rapporto di lavoro

Garantire gli aspetti di sicurezza nel processo di variazione o di cessazione del rapporto di lavoro.

Particolare attenzione deve essere posta nella cessazione del rapporto di lavoro dove specifici processi e procedure devono essere predisposte per garantire gli aspetti di sicurezza.

Gestione degli asset

Responsabilità per gli asset

Identificare ed assegnare specifiche responsabilità per tutti gli asset in ambito sicurezza delle informazioni.

Classificazione delle informazioni

Garantire un adeguato livello di protezione alle informazioni.

Le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità.

Trattamento dei supporti

Evitare che le informazioni archiviate sui supporti vengano divulgate, modificate, rimosse o eliminate senza la corretta autorizzazione.

Deve essere applicato il corretto livello di protezione in base alla classificazione delle informazioni.

Controllo degli accessi

Gestione degli accessi

Garantire l'accesso ai sistemi ai soli utenti autorizzati

Devono essere applicati i seguenti principi generali per garantire l'obiettivo ponendo particolare attenzione alla concessione ed alla revoca delle credenziali e dei privilegi di accesso:

- l'accesso ed il possesso di privilegi devono essere limitati alle sole informazioni strettamente necessarie per l'esecuzione delle mansioni assegnate;
- per ridurre la possibilità di uso improprio degli asset contenenti informazioni, le modalità di accesso ed i ruoli devono essere formalizzati.

Informazioni di autenticazione gestite dagli utenti

Responsabilizzare gli utenti nella gestione/utilizzo di utenza e password.

Controllo accesso ai sistemi informatici

Consentire accesso ai soli utenti autorizzati a sistemi e applicazioni non autorizzato.

Crittografia

Controlli

Garantire un uso corretto della crittografia per la protezione delle informazioni.

L'utilizzo della crittografia deve avvenire in accordo a normative, adempimenti contrattuali ed a requisiti specifici per la protezione dei dati. In particolare, si deve proteggere la riservatezza, l'integrità ed il non ripudio delle informazioni.

Chiavi crittografiche

Garantire una corretta gestione delle chiavi.

Sicurezza fisica e ambientale

Garantire accesso fisico ai sistemi ed alle informazioni ai soli utenti autorizzati.

Attività operative

Procedure e responsabilità

Garantire la sicurezza delle informazioni durante le attività operative.

Le procedure operative, necessarie per l'esecuzione delle attività che includono gli aspetti relativi alla sicurezza devono essere adeguatamente predisposte.

Malware

Garantire la sicurezza delle informazioni (e dei sistemi) contro il malware.

Backup

Garantire l'integrità e la disponibilità dei dati.

Oggetto del backup sono principalmente: dati, log, configurazioni (sistemi e rete), sistemi operativi e software.
L'integrità e la disponibilità delle informazioni sono garantite tramite l'utilizzo di strumenti e procedure per il backup ed il ripristino dei dati.

Vulnerabilità

Prevenire lo sfruttamento di vulnerabilità tecniche.

L'esposizione a vulnerabilità tecnica deve essere valutata tempestivamente per abilitare contromisure opportune in moda da ridurre ed eliminare i relativi rischi.

Comunicazioni

Sicurezza della rete

Garantire la protezione delle informazioni nelle reti (inclusi gli apparati a supporto).

Trasferimento delle informazioni

Mantenere la sicurezza delle informazioni trasferite internamente ed esternamente all'azienda.

Devono essere previsti opportuni accordi di riservatezza. Tali accordi devono essere revisionati periodicamente.

Acquisizione, sviluppo e manutenzione di sistemi e applicazioni

Requisiti di sicurezza di servizi ed applicazioni

Garantire la sicurezza delle informazioni per tutto il ciclo di vita di servizi ed applicazioni.

Processi di sviluppo e supporto

Garantire la sicurezza delle informazioni per le fasi di sviluppo e supporto.

Dati da usare in fase di test

Garantire la protezione dei dati usati per il test.

Gestione fornitori

Relazioni con i fornitori

Garantire la sicurezza delle informazioni assicurando la protezione degli asset.

I requisiti relativi alla sicurezza delle informazioni devono essere stabiliti, concordati e documentati negli accordi con ciascun fornitore che tratta informazioni dell'azienda o dei Clienti. In caso di filiera, gli accordi appena citati devono essere opportunamente estesi.

Servizi erogati da fornitori

Garantire la sicurezza delle informazioni attraverso monitoraggio dei livelli di sicurezza offerti (in accordo con i contratti di fornitura).

Incidenti di sicurezza

Gestire in modo efficace gli incidenti di sicurezza.

Le responsabilità e le procedure di gestione devono essere identificate per assicurare una risposta rapida ed efficace nella gestione degli incidenti di sicurezza.

Continuità operativa

Assicurare la disponibilità dei sistemi.

Processi, procedure e controlli devono essere stabiliti, documentati, attuati per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.

Conformità

Assicurare la conformità con norme e requisiti contrattuali in merito alla sicurezza delle informazioni.

Revisione della politica di sicurezza

Assicurare l'applicabilità e l'utilità della politica di sicurezza.

Miglioramento continuo

Assicurare il miglioramento continuo del SGSI.

GSA si impegna a mantenere e migliorare continuamente il sistema di gestione per la sicurezza delle informazioni (SGSI) in conformità con la norma ISO 27001:2022. A tal fine, GSA oltre a verificare costantemente la validità di tutti gli obiettivi precedenti e, in particolare, promuovere la consapevolezza e la formazione del personale sulle questioni di sicurezza, prevede i seguenti meccanismi per gestire il miglioramento:

- feedback di clienti, fornitori e delle altre parti interessate per valutare spazi di miglioramento non evidenziati internamente;
- osservazione continua di cambiamenti tecnologici, normativi e di mercato che possono influire sul SGSI;
- verifica periodica della conformità con i requisiti legali e contrattuali applicabili.

La Direzione
GESTIONE SERVIZI AZIENDALI S.r.l.
LA DIREZIONE
(Dott. Nicola Paoletti)