REQUISITI GENERALI DI SICUREZZA INFORMATICA

DIREZIONE SISTEMI INFORMATIVI E SERVIZI

Sommario

1 Ambito e finalità del documento

In questo documento, sono descritte le pratiche minime richieste agli Appaltatori nelle loro interazioni con i servizi e le risorse digitali del GSE conseguenti la stipula di un contratto, ai fini di una corretta gestione delle tematiche di sicurezza sia nel caso in cui il personale degli Appaltatori è direttamente connesso alla rete GSE, sia quando opera in modalità remota utilizzando connessioni telematiche verso i sistemi GSE da propri client (per esempio tramite VPN).

2 Riferimenti normativi

Con la sottoscrizione del contratto l'Appaltatore dichiara espressamente di aver preso piena conoscenza delle disposizioni e norme di sicurezza di seguito elencate e adottate dalla Società, volte ad aumentare il livello di sicurezza delle infrastrutture e dei servizi digitali in conformità alle seguenti normative:

- CAD, Codice dell'Amministrazione Digitale – Decreto Legislativo n.82 del 7 marzo 2005;
- GDPR, General Data Protection Regulation - Regolamento UE 2016/679;
- Provvedimento del 2 luglio 2015 - Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche (Garante per la Protezione dei Dati Personali);
- Provvedimento del 27 novembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministrazione di sistema (Garante per la Protezione dei Dati Personali);
- Misure minime di sicurezza ICT per le Pubbliche Amministrazioni (AgID - Agenzia per l'Italia Digitale).

3 Prescrizioni emanate col presente documento

L'Appaltatore è tenuto a informare le proprie risorse (dipendenti/ consulenti/ collaboratori) che svolgono la loro attività sia presso le sedi aziendali che in modalità remota circa le condizioni e i limiti di seguito elencati, entro i quali possono legittimamente utilizzare le postazioni di lavoro proprie o assegnate dal GSE, i servizi Internet/ intranet e ogni altro eventuale strumento o dispositivo informatico e telematico messo a disposizione, nonché la modalità e le condizioni di accesso ai sistemi e ai servizi informatici del GSE.

Coerentemente con il Principio di privacy by design, introdotto dall'art.25 del GDPR in merito alla tutela del patrimonio informativo aziendale, l'Appaltatore è tenuto ad adottare le misure di sicurezza in tutte le fasi del ciclo di vita dei sistemi/ applicazioni informatici del GSE attraverso cui si realizza un trattamento dei dati, al fine di assicurare che le iniziative di progettazione, sviluppo, realizzazione, gestione ed evoluzione di un sistema informatico siano svolte nel rispetto del Provvedimento in materia di protezione di dati Personali GDPR.

4 Credenziali di accesso a risorse e loro utilizzo

L'utilizzo delle risorse del GSE è vincolato strettamente all'esercizio delle attività lavorative e non è consentito per usi personali, pertanto si ha l'obbligo di custodire e mantenere in buono stato le risorse informatiche concesse dal GSE, disconnettere gli applicativi in uso ogniqualvolta ci si allontani dalla postazione utilizzando anche le funzionalità offerte dal sistema operativo ("blocca computer"), contribuendo a garantire la disponibilità e l'integrità dei dati trattati.

Il GSE attua un controllo degli accessi logici per i propri sistemi informatici attraverso il riconoscimento dell'identità del soggetto autorizzato ad accedere ad una risorsa informativa del GSE. Tale controllo è eseguito a partire dalla definizione dell'Identità Digitale, da intendersi come l'insieme dei dati che permettono di contraddistinguere univocamente un soggetto per la determinazione dei relativi diritti di accesso a una risorsa informativa.

Le credenziali di accesso rilasciate dal GSE sono costituite da un codice utente e da un fattore di autenticazione da non divulgare. Per aumentare il livello di sicurezza dei servizi esposti sul perimetro, potrà essere aggiunto un secondo fattore di autenticazione, per l'utilizzo del quale potrebbe essere richiesta l'installazione di uno specifico software o agent sul dispositivo mobile dell'utente che richiede accesso ai servizi informativi di GSE.

Le credenziali di accesso per i sistemi informatici del GSE sono personali e associate a un'identità digitale, in modo che le azioni eseguite siano riconducibili al soggetto assegnatario. Quest'ultimo è tenuto a proteggere e mantenere riservate le proprie credenziali, segnalando tempestivamente al GSE eventuali furti o riscontri di anomalie di accesso.

Nella scelta del fattore di autenticazione occorre seguire le regole utilizzate in GSE, in particolare evitando parole comuni o nomi propri, date e altri dettagli personali, e scegliendo almeno 14 caratteri fra i quali figurino maiuscole, minuscole, cifre e caratteri speciali. La validità del fattore di autenticazione è di 90 giorni. Per la modifica della password è preferibile utilizzare più variazioni alfanumeriche mentre alla scadenza è obbligatorio non inserire le ultime 14 password precedentemente utilizzate. Infine le stesse non devono essere inserite nei messaggi di posta elettronica o trasmesse attraverso altra forma di comunicazione e/o inserite all'interno di programmi o script.

5 Procedura di accesso da una postazione del GSE

L'accesso alla rete Intranet del GSE è possibile solo da postazione dedicata fornita dal GSE e opportunamente collegata in rete tramite cavo ethernet e non potrà essere spostata dal punto di rete cui è collegata al momento della consegna da parte del GSE al personale dell'Appaltatore.

Il personale dell'Appaltatore accederà tramite la propria utenza GSE e non potrà collegare dispositivi di rete o di storage alla postazione se non forniti dal GSE.

I dispositivi client connessi alla rete aziendale non possono essere connessi simultaneamente ad altre reti dati (es: Tethering, WiFi, Bluetooth) e/o più in generale non è consentito l'impiego di funzionalità per anonimizzare il proprio accesso.

Non sono consentiti accessi remoti alla rete aziendale GSE mediante servizi wireless di *hot-spot* pubblici per i quali non è garantita alcuna forma di riservatezza e protezione delle comunicazioni.

6 Procedura di accesso da una postazione remota

È possibile collegare una postazione di terzi solo da remoto tramite VPN e se conforme ai seguenti requisiti minimi:

- Sistema Operativo dotato di licenza originale ed ufficialmente supportato dal relativo brand, con un adeguato livello di patching di sicurezza;
- Sistema Antivirus dotato di licenza originale ed aggiornato;
- Browser Internet aggiornati e supportati al fine di garantire la sicurezza della navigazione;
- Navigazione Internet controllata da strumenti che garantiscono la navigazione sicura (Proxy, Software Client per la Navigazione Sicura);

In particolare, l'accesso remoto all'intranet aziendale è consentito esclusivamente con connessioni protette VPN da postazioni di lavoro che prevedano la rispondenza ai requisiti minimi di sicurezza richiesti, in accordo con la seguente procedura:

1. Installazione del client VPN fornito dal GSE;
2. Implementazione dei seguenti controlli sulla postazione:
    - mac address della postazione;
    - autenticazione con Multi Factor Authentication (MFA);
    - controllo presenza antivirus;
    - controllo attivazione windows update.
3. L'accesso sarà consentito ai soli servizi necessari per l'operatività.

I dispositivi client connessi remotamente alla rete aziendale non possono essere connessi simultaneamente ad altre reti dati (es: Tethering, WiFi, Bluetooth) oltre a quella utilizzata per la VPN e/o più in generale non è consentito l'impiego di funzionalità per anonimizzare il proprio accesso.

Non sono consentiti accessi remoti alla rete aziendale GSE mediante servizi wireless di *hot-spot* pubblici per i quali non è garantita alcuna forma di riservatezza e protezione delle comunicazioni.

Eventuali collegamenti remoti, aventi caratteristiche di permanenza, tra l'infrastruttura ICT dell'Appaltatore e di GSE (VPN Site-to-Site) devono essere formalmente approvati dalle strutture competenti di GSE a seguito di una valutazione dei rischi e della sottoscrizione di un accordo di interconnessione, o analogo protocollo

d'intesa, che stabilisca le reciproche responsabilità per la sicurezza dell'interconnessione e documenti le misure di protezione.

Il GSE si riserva il diritto di inibire l'accesso alla rete aziendale a sistemi di terze parti non osservanti i requisiti minimi indicati ai precedenti punti e/o coinvolti in comportamenti anomali e/o incidenti di sicurezza che impattano l'infrastruttura e i sistemi ICT del GSE.

7 Servizi Internet

La navigazione internet dalla rete GSE è consentita esclusivamente tramite *proxy*, impostato nel *browser* secondo le configurazioni fornite dal GSE, e deve essere finalizzato a scopi esclusivamente lavorativi.

Il GSE periodicamente procederà, nel rispetto delle garanzie di tutela dei dati personali previste dalla normativa vigente, ad un controllo qualitativo dell'utilizzo della rete Internet per verificarne la conformità alle politiche aziendali.

L'infrastruttura di rete GSE filtra i contenuti accessibili su Internet dalla propria rete e in particolare:

- non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica e comunque con contenuti di natura illegale o in contrasto con il codice etico aziendale;
- non è consentito l'accesso e l'utilizzo di sistemi e/o servizi che permettano l'elusione dei controlli da parte dei sistemi aziendali: la comunicazione o l'invio di dati e/o documenti aziendali deve essere effettuata nel rispetto delle procedure interne e mediante i canali di comunicazione aziendalmente abilitati;
- non è consentito scaricare e/o installare software non espressamente autorizzati dalle strutture competenti di GSE e per i soli fini legati all'attività lavorativa;
- non è consentito scaricare video, brani musicali, giochi e materiale coperto dal diritto d'autore;
- non è consentito lo scambio a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico ecc., protetto da copyright.

8 Uso della posta elettronica GSE

La posta elettronica messa a disposizione da GSE (ove previsto) rappresenta uno strumento di proprietà aziendale per lo svolgimento delle attività lavorative, pertanto è responsabilità dell'utente garantire riservatezza delle password di accesso nonché il corretto utilizzo dello stesso. Di conseguenza non è possibile inviare o memorizzare messaggi che non rispettino la normativa vigente in materia (es: messaggi di natura oltraggiosa, volgare e/o discriminatoria) o per scopi che esulano dall'espletamento delle mansioni affidate.

È necessario prestare attenzione nell'utilizzo della posta elettronica segnalando messaggi e mittenti sospetti tramite gli appositi strumenti indicati dal GSE, evitando l'apertura di allegati e/o link di cui non si è certi della sicurezza.

Infine si precisa che in casi specifici e in conformità con la legislazione vigente, su esplicita richiesta dell'Autorità Giudiziaria competente, le e-mail memorizzate nei sistemi del GSE potrebbero essere eventualmente fornite alle predette autorità.

9 Comportamenti prescritti nell'utilizzo della postazione GSE

L'utente deve prestare assoluta attenzione a non lasciare mai incustodita alcuna strumentazione o apparecchiatura assegnategli dal GSE (ove previsto) e a prendere tutte le precauzioni affinché non vengano smarrite, danneggiate o rubate anche al di fuori dalle sedi aziendali. Nel caso si dovesse verificare un furto o danneggiamento, il GSE deve essere tempestivamente informato dell'accaduto e deve essere presentata immediatamente denuncia presso le autorità competenti.

Ogni postazione fornita dal GSE (ove previsto) è corredata da software antivirus aziendale adeguatamente configurato ed aggiornato. È vietato disattivare l'antivirus, modificarne la configurazione o installare ulteriori antivirus o software non autorizzati. Prima di caricare un qualunque tipo di dato o programma da supporto esterno deve essere effettuata la scansione utilizzando l'antivirus messo a disposizione dal GSE. In caso di rilevazione e mancata eliminazione del virus deve essere scollegata la postazione dalla rete e segnalato tempestivamente l'accaduto alle strutture competenti di GSE fornendo tutti i dati.

È proibito cifrare, trasmettere, o salvare le informazioni del GSE di qualsiasi natura, in assenza di esplicita autorizzazione da parte delle strutture competenti di GSE che monitorano costantemente i sistemi informatici in conformità con la legislazione vigente.