Requisiti generali di sicurezza informatica

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 ed adottate dalla Società, volte ad aumentare il livello di sicurezza delle infrastrutture e dei servizi digitali in conformità ai seguenti requisiti normativi:

- GDPR, General Data Protection Regulation - Regolamento UE 2016/679,
- Provv. 02/07/2015 - Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche (Garante Privacy),
- Provv. 27/11/2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministrazione di sistema (Garante Privacy),
- AgID - Misure minime di sicurezza ICT per le Pubbliche Amministrazioni;
- C.A.D. – Codice dell'Amministrazione Digitale.

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.

Principi generali di Sicurezza Informatica per lo svolgimento dei Servizi

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

- l'utilizzo delle risorse aziendali è vincolato strettamente all'esercizio delle attività lavorative e non 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 ed integrità dei dati trattati. Nel caso di utilizzo improprio o difforme da quanto indicato è necessario segnalare l'accaduto a GSE;
- il GSE attua un controllo degli accessi logici per i propri sistemi informatici attraverso il riconoscimento dell'identità del soggetto che necessita ed è autorizzato ad accedere ad una risorsa informativa del GSE. Tale controllo è eseguito 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 ad una risorsa informativa;

- le credenziali di accesso rilasciate dal GSE sono generalmente costituite da un codice utente univoco (detto UserID o anche utenza o username) e da un fattore di autenticazione, tipicamente una parola chiave segreta, la cosiddetta password. In alcuni casi, per aumentare il livello di Sicurezza dei servizi esposti sul perimetro, il GSE adotta meccanismi basati su un secondo fattore di autenticazione, costituito ad esempio da un dispositivo che si possiede come una smartcard o un token OTP (di tipo fisico o virtuale) per l'utilizzo del quale potrebbe essere richiesta l'installazione di uno specifico software o agent sul dispositivo terminale dell'utente che richiede accesso ai servizi informativi di GSE;
- le credenziali di accesso per i sistemi informatici del GSE sono personali e associate ad un'identità digitale, pertanto tutte le azioni eseguite in tale ambito sono riconducibili al soggetto assegnatario che ha l'obbligo di non condividere e proteggere con particolare cura le proprie credenziali segnalando tempestivamente al GSE eventuali furti o riscontri di anomalie di accesso, per evitare che possano essere attribuite in modo non appropriato eventuali azioni dannose o addirittura dolose commesse tramite di esse;
- nel rispetto esplicito delle regole utilizzate in GSE nella gestione delle proprie credenziali, per la scelta della password è vietato inserire dettagli personali mentre è obbligatorio l'uso di almeno 8 caratteri alfanumerici contenente sia lettere maiuscole/minuscole/numeri e preferibilmente caratteri speciali e con validità massima di 90 gg. Per la modifica della password è preferibile utilizzare più variazioni alfanumeriche mentre alla scadenza è obbligatorio non inserire le ultime 10 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;
- l'utilizzo dei servizi internet del GSE è consentito previa autenticazione con codice identificativo e password. È espressamente vietato condividere ed utilizzare le credenziali di altri utenti per accedere ad internet. L'utilizzo del collegamento aziendale è consentito tramite proxy e deve essere finalizzato a scopi esclusivamente lavorativi. Inoltre non è consentito connettere gli strumenti informatici aziendali o comunque dispositivi connessi alla rete GSE, a reti esterne pubbliche o private per mezzo di collegamenti fisici con linee dati dedicate o tramite reti di telefonia mobile / strumenti wireless di qualsiasi genere senza un'esplicita autorizzazione. Infine 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;
- il GSE, a tutela del proprio patrimonio informativo aziendale, opera un filtro dei contenuti accessibili dalla propria intranet mediante Internet. 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 l'utilizzo di piattaforme di File Sharing, piattaforme di Collaboration o altri sistemi di tipo Cloud Based, che comportino la condivisione di file o altro contenuto di interesse aziendale se non espressamente autorizzate dalle strutture competenti di GSE e per i soli fini legati all'attività lavorativa;
- non è consentito scaricare software gratuiti (freeware e shareware) prelevati da siti Internet, se non espressamente autorizzati dalle strutture competenti di GSE e per i soli fini legati all'attività lavorativa. È, altresì, proibito scaricare video, brani musicali, giochi e materiale coperto dal diritto d'autore; non è consentito lo scambio (ad esempio Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright;

- i servizi di connettività wireless di ogni tipo disponibili su computer fissi o portatili devono essere disabilitati quando connessi alla rete aziendale in modalità "*wired*";
- sono ammesse, previa autorizzazione del GSE, connessioni realizzate mediante tecnologia di tipo wireless messa a disposizione dal GSE all'interno delle proprie sedi, esclusivamente per l'accesso alla rete Internet, in modalità cifrata e autenticata;
- non sono consentiti accessi remoti alla rete aziendale GSE mediante servizi wireless di HotSpot pubblici per i quali non è garantita alcuna forma di riservatezza e protezione delle comunicazioni;
- 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 di natura oltraggiosa, volgare e/o discriminatoria o per scopi che esulano dall'espletamento delle mansioni affidate. È necessario fare attenzione alla posta ricevuta controllando gli allegati, gli eventuali link presenti nel corpo della mail, eliminando i messaggi insoliti o di mittenti sconosciuti. Infine si precisa che in casi specifici ed in conformità con la legislazione vigente, su esplicita richiesta dell'Autorità Giudiziaria competente, le e-mail memorizzate nei sistemi del GSE potrebbero essere eventualmente divulgate o rese note alle predette autorità;

- 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, quali l'utilizzo di un sistema operativo supportato ed adeguatamente aggiornato con le relative patch di sicurezza e la presenza di un sistema antivirus aggiornato. Nel caso specifico di smartphone e /o tablet, non è consentito l'accesso da parte di dispositivi rooted o sottoposti a jailbreak;
- eventuali eccezioni a quanto indicato al precedente punto, quali l'impiego di Strumenti di *collaboration* aziendali o l'impiego di tecnologie di connessione remota alternative, dovranno essere puntualmente verificate ed eventualmente autorizzate dalle strutture competenti del GSE, previa verifica del rispetto degli analoghi requisiti di sicurezza;
- i dispositivi client connessi remotamente alla rete aziendale non possono essere connessi simultaneamente ad altre reti dati (bridging) e/o più in generale non è consentito l'impiego di funzionalità quali "split tunneling" o tecniche di "Proxy anonimo";
- è consentito, previa autorizzazione del GSE, l'accesso remoto da ambienti/contesti virtuali che realizzino una opportuna segregazione delle comunicazioni/dati aziendali veicolate tramite VPN dal sistema client o altro meccanismo che permetta un tunnel cifrato ed autenticato tale da garantire un adeguato livello di riservatezza ed integrità delle comunicazioni;
- l'accesso remoto all'intranet aziendale deve avvenire, per quanto possibile, con dotazioni informatiche fornite dall'Azienda. Tuttavia nel caso di reale e comprovata necessità di accedere alle risorse aziendali, è possibile utilizzare pc di terzi, che verifichino i requisiti di minimi sicurezza di cui la punto seguente, attenendosi rigorosamente alle norme comportamentali indicate nel presente documento;
- nel caso di collegamento on-site e/o diretto alla rete GSE, da parte di dispositivi non forniti da GSE, l'attestazione dovrà avvenire su reti dedicate e/o opportunamente segregate. Non sarà comunque possibile collegare alla rete aziendale (in locale e/o da remoto) pc di terzi che non siano dotati dei seguenti requisiti minimi indicati: 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 dal brand al fine di garantire la sicurezza negli accessi remoti con tecnologia VPN SSL e alla rete Internet.
- eventuali collegamenti remoti, aventi caratteristiche di permanenza, tra l'infrastruttura ICT del fornitore e di GSE (VPN Site-to-Site) devono essere conformi ai seguenti requisiti:

    - devono essere realizzati con modalità conformi al framework IPSec garantendo la cifratura e l'inalterabilità dei flussi informativi;

- devono essere formalmente approvati dalle strutture competenti di GSE, prima dell'attivazione, a valle di una valutazione dei rischi e della sottoscrizione di un accordo di interconnessione - o un analogo protocollo d'intesa - che stabilisca le reciproche responsabilità per la sicurezza dell'interconnessione e documenti le misure di protezione;

- il GSE, per tutte le connessioni in modalità VPN, si riserva di verificare se installare sui dispositivi opportuni agent per l'utilizzo della VPN tramite un sistema client, o di consentire l'utilizzo della VPN in modalità SSL. Il GSE si riserva, inoltre, il diritto di inibire l'accesso alla rete aziendale (in locale e/o da remoto) a sistemi di terze parti non osservanti i requisiti minimi indicati ai precedenti punti e/o coinvolti in incidenti di sicurezza inerenti l'infrastruttura ed i sistemi ICT del GSE;
- l'utente deve prestare assoluta attenzione a non lasciare mai incustodita alcuna strumentazione o apparecchiatura assegnatigli dal GSE (ove previsto) e devono essere prese 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 prontamente informato dell'accaduto e deve essere presentata tempestiva denuncia presso le autorità competenti;
- ogni personal computer fornito dal GSE (ove previsto) è corredato di software antivirus aziendali adeguatamente configurati ed aggiornati. 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 dell'Azienda. In caso di rilevazione e mancata eliminazione del virus deve essere sospesa l'attività lavorativa e segnalato 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;
- il GSE opera il monitoraggio degli accessi logici ai propri sistemi informatici in conformità con la legislazione vigente. Per quanto attiene alle attività svolte con privilegi ammnistrativi, sono tracciati l'accesso, le attività svolte e l'uscita dai sistemi di GSE nonché i riferimenti temporali delle suddette attività. Tali informazioni o dati raccolti sono acquisiti ed archiviati, con opportune misure di sicurezza, nei limiti sanciti dalla normativa vigente e sono trattati in via eccezionale per richieste della polizia giudiziaria e/o dell'autorità giudiziaria, oppure quando sia necessario condurre attività di analisi a seguito di anomalie e/o malfunzionamenti di sistema.

Qualora il contratto preveda che l'Appaltatore amministri sistemi informatici del GSE, l'Appaltatore medesimo è tenuto, ai sensi della suddetta normativa (Provv. 27/11/2008), a nominare formalmente quali "Amministratori di Sistema" i propri collaboratori che, nell'ambito delle attività contrattuali previste, operino con profili

amministrativi sui sistemi informatici del GSE, fornendo opportuna comunicazione al GSE dell'avvenuta nomina. Si precisa che è responsabilità dell'appaltatore revocare oppure adeguare l'ambito della suddetta nomina (fornendo opportuna comunicazione al GSE) in caso di variazioni organizzative che comportino una modifica delle mansioni della risorsa operante presso GSE.

Comunicazione e segnalazione degli incidenti di sicurezza informatica

L'Appaltatore nell'ambito dello svolgimento delle proprie attività attraverso l'utilizzo dei sistemi informativi del GSE è tenuto ad informare tempestivamente l'Azienda qualora si verificassero le condizioni per un mancato rispetto dei requisiti di sicurezza informatica riportati nel presente documento e comunque al verificarsi di qualsiasi comportamento da parte dei propri collaboratori che potrebbe compromettere in qualsiasi misura la riservatezza, l'integrità e la disponibilità dei sistemi e del patrimonio informativo del GSE.

Tali comunicazioni devono pervenire tempestivamente al GSE tramite i canali messi a disposizione in fase di contrattualizzazione del servizio/fornitura al fine di permettere le opportune analisi, stabilire la gravità ed avviare eventuali provvedimenti ed azioni di contenimento e/o risoluzione della problematica. Tutte le segnalazioni o comunicazioni che saranno riconducibili ad un incidente di sicurezza informatica e relative alla violazione di uno o più requisiti descritti nel presente documento, saranno tracciati dal GSE secondo le modalità previste ed in conformità delle policy aziendali.

In tutti i casi l'Appaltatore dovrà rendersi disponibile e fornire tutte le informazioni necessarie per le valutazioni di impatto e gravità dell'accadimento sui sistemi ed il patrimonio informativo del GSE eventualmente coinvolto.