REGOLAMENTO IT

Data rilascio documento: 23/09/2019	Data prima approvazione:	Data ultima modifica: [Vedi tabella di controllo versioni]	Data prossima Review:
Prima approvazione da parte di:			
Gestione progetto e custode documentazione:			
Autori:	Francesco Moroncini - DPO ASUR M. Teresa Guiducci Dirigente Analista SIA ASUR Ebe Tartufo – Assistente Tecnico Programmatore SIA ASUR		
Responsabile della UO:	Sergio Piersantelli - Direttore Dipartimento Sistemi Informativi ASUR		
Documenti di supporto, Procedure e modulistica:	<link al repository> Procedure <Modulistica di supporto>		
Legislazione rilevante in materia:	<link>		
Audience:	Dipendenti e fornitori		

Il presente Regolamento deve necessariamente adattarsi alla continua evoluzione normativa, alle nuove tecnologie e ai nuovi dispositivi che potranno essere introdotti in futuro nell'organizzazione; per questo motivo i lettori sono invitati a segnalare eventuali inesattezze, modifiche o integrazioni che si rendessero necessarie utilizzando l'indirizzo e-mail di seguito riportato:

sistemiinformativi.asur@sanita.marche.it

Controllo versione e Cronologia modifiche

Controllo di versione	Data effettiva	Approvato da	Descrizione delle modifiche effettuate
1.0	05/09/2019		Versione preliminare
1.1	23/09/2019		Prima revisione del Regolamento
1.3	2/12/2019		Seconda revisione del Regolamento
1.4	07/01/2020		Ultima revisione prima della pubblicazione

In copertina la Stele di Rosetta (196 a.C.) British Museum, Londra

Chiave decisiva per la comprensione dei geroglifici egizi

Sommario

Introduzione

Le pubbliche amministrazioni raccolgono, organizzano e gestiscono una vasta quantità di dati, personali e non. Tuttavia, negli anni, l'autonomia delle singole amministrazioni e le modalità di gestione dei dati hanno contribuito a creare delle isole di informazioni contenute principalmente in archivi digitali (basi di dati informatizzate, procedure e programmi software, condivisioni di rete) ma anche in archivi analogici (dati cartacei) e spesso anche all'interno di caselle di posta elettronica, negli smartphone e nei programmi di instant messaging (come WhatsApp, WeChat, Facebook Messenger), apertissimi anche alla gestione degli allegati per ovvie finalità di raccolta.

Tali dati costituiscono il così detto patrimonio informativo dell'azienda, dal valore strategico ed economico inestimabile nell'attuale società delle informazioni, poiché ASUR Marche è un'azienda sanitaria di livello regionale con un bacino di utenza di più di un milione di persone.

Il rapporto Clusit 2019 (Associazione Italiana per la Sicurezza Informatica) conferma che gli attacchi informatici sono in crescita soprattutto in ambito sanitario. Truffe ed estorsioni realizzate tramite tecniche di phishing e ransomware, hanno colpito moltissime organizzazioni e cittadini italiani; questa tipologia di attacchi con finalità di estorsione o sottrazione di informazioni (rappresentano l'85% degli attacchi a livello globale e la tendenza è in crescita) non solo comporta un immediato ed evidente danno economico ma ha, o rischia di avere, effetti collaterali pesantissimi in termini di continuità di servizio, problema questo particolarmente sentito in sanità per gli evidenti risvolti sulla salute stessa dei pazienti.

La crescita dell'uso di tecniche di phishing e social engineering per compiere con successo attacchi gravi ci conferma ancora una volta quanto sia fondamentale ed urgente investire in misure tecniche ed organizzative finalizzate alla protezione dei dati e dei sistemi informatici in particolare.

Il presente regolamento, come illustrato più avanti, vuole essere uno strumento sia di organizzazione che di divulgazione tecnologica e normativa, poiché è la consapevolezza degli utilizzatori il primo elemento di prevenzione.

Gli strumenti e i servizi aziendali forniti al lavoratore, quali Personal Computer, Notebook, Tablet, Smartphone, e-mail, connessione Internet e tutti gli altri necessari dispositivi hardware (server, apparati di rete: router, switch, hotspot, ecc.) e software, di seguito più semplicemente "strumenti informatici", sono messi a disposizione dei dipendenti e dei collaboratori unicamente per svolgere la propria attività lavorativa.

Nell'utilizzare tale strumenti informatici, tutti sono tenuti ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile, servendosene esclusivamente per ragioni di servizio e nel rispetto delle indicazioni contenute nel presente Regolamento, il cui scopo è quello delineare i comportamenti consentiti, consigliati o da evitare perché a volte, anche inconsapevolmente, si possono innescare attività rischiose e minacce alla sicurezza del sistema informatico.

Comportamenti difformi da quanto indicato nel presente Regolamento possono contribuire ad innescare disservizi, causare gravi rischi all'integrità e alla disponibilità delle informazioni, dei servizi e degli strumenti informatici.

Premessa

Con il termine I*nformation Security (*Sicurezza Informatica) intendiamo l'insieme degli strumenti e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, riservatezza e integrità dei dati, dei servizi e degli strumenti informatici.

La protezione degli strumenti e dei sistemi *ICT* (*Information and Communication Technology*) passa prima di tutto attraverso la consapevolezza degli operatori su quali siano le minacce, le vulnerabilità e i rischi che incombono su di essi, al fine prevenire possibili attacchi (interni o esterni, dolosi o involontari) che potrebbero provocare danni diretti o indiretti, con un impatto superiore a una determinata soglia di tollerabilità

L'analisi del rischio è lo strumento principale per evidenziare ed esplicitare le minacce ed è il punto di partenza per avere consapevolezza sulla propria reale situazione e per introdurre, adeguare o aggiornare le misure tecniche ed organizzative necessarie a raggiungere un livello di sicurezza adeguato in relazione ai rischi evidenziati.

Nella gestione della sicurezza informatica sono coinvolti molteplici elementi: tecnologici, organizzativi, giuridici e umani. Le misure per attenuare i danni e ridurre il rischio di perdita, manipolazione o sottrazione di dati, prevedono un puntuale e rigido controllo degli accessi, (utilizzo di strumenti che regolamentino gli accessi alle procedure e ai servizi ICT, identificazione nominativa degli operatori, regolamentazione dell'utilizzo e monitoraggio delle attività svolte) una corretta e precisa profilazione degli utenti (pertinenza e non eccedenza rispetto ai compiti e competenze di ognuno) ma soprattutto una formazione continua e pressante sugli operatori (aumento delle competenze, diffusione di *best practice* e sensibilizzazione rispetto all'argomento) in quanto sono proprio loro l'anello debole della catena che sempre più spesso con comportamenti superficiali o involontari provocano danni (diffusione di *worm* e virus provenienti da e-mail infette, adescamento tramite *phishing*).

Anche la progettazione e la scelta del software deve essere ponderata in quanto gli applicativi utilizzati devono rispettare adeguati standard di qualità (es. Norme AgID sul Cloud per la PA, protocollo SSL, strumenti di autenticazione forte, …) al fine di garantire un auspicato contenimento delle vulnerabilità legate al codice sorgente (GDPR art. 25 - Privacy by design e privacy by default). Il costante aggiornamento dei software (sistemi operativi, antivirus e programmi in generale) è un elemento essenziale per garantire un'adeguata protezione al continuo evolversi delle minacce e delle vulnerabilità.

Se si considera che la maggior parte degli attacchi e quindi dei problemi sono provocati dagli stessi dipendenti delle organizzazioni, spesso in modo inconsapevole e involontario, si comprende come l'adozione di una regolamentazione sia a tutti gli effetti un intervento più culturale che normativo (Principio di *Accountability* ovvero di responsabilizzazione)

L'obiettivo del presente regolamento, insieme ai percorsi di formazione che ASUR ha pianificato e predisposto, è quello di sensibilizzare, responsabilizzare e accrescere le competenze dei singoli individui, al fine di aumentare le competenze finalizzate a prevenire comportamenti potenzialmente pericolosi che espongono tutta l'organizzazione a rischi che potrebbero sfociare anche in sanzioni, risarcimenti o peggio ancora a danni reputazionali e/o di immagine.

Approccio metodologico

L'obiettivo di un qualunque ***Regolamento*** è la definizione delle modalità di funzionamento di un sistema organizzativo o tecnologico e la relativa disciplina di utilizzo.

Solitamente vengono prima declinati i principi generali che hanno richiesto o suggerito la regolamentazione, a cui segue parte attuativa e l'immancabile parte relativa alle sanzioni con gli allegati utili nella comprensione dell'applicazione pratica.

La redazione di un ***Regolamento per l'utilizzo di sistemi e di servizi IT ha come obiettivo primario la definizione delle politiche di sicurezza*** dell'organizzazione in modo da disciplinare:

- le cose che si *possono* fare;
- le cose che si *devono* fare secondo una specifica procedura;
- quanto *non è* proprio possibile fare.

Da un lato l'organizzazione ha la necessità di normare questo ambito per tutelare il suo patrimonio informativo e per prevenire problemi reputazionali o danni di immagine dovuti ad utilizzi impropri degli strumenti; dall'altro deve sensibilizzare, formare ed informare il personale su tematiche sempre nuove legate al progresso e all'innovazione che, considerati i ritmi evolutivi, crea dei veri e propri dislivelli culturali difficilmente colmabili.

La regolamentazione che segue modifica radicalmente l'approccio tradizionale, introducendo una metodologia più rigorosa e basata sull'analisi dei rischi che incombono sull'organizzazione e sui sistemi informatici.

In modo forse non canonico ma funzionale, si è partiti dalle sorgenti di dati, analizzando le potenziali minacce e vulnerabilità, integrando progressivamente con casistiche basate su eventi realmente accaduti.

In altre parole, pur mantenendo l'asse sui principi generali, il focus è rivolto alla costruzione di uno strumento che possa fungere da vademecum, con l'obiettivo di educare gli utilizzatori ad un uso consapevole e corretto piuttosto che un mero dispositivo normativo di repressione delle cattive pratiche.

L'intento è quindi quello di avviare un'azione di sensibilizzazione, che incrementi le conoscenze legate agli strumenti tecnologici e ai rischi connessi, al fine di attivare una nuova consapevolezza finalizzata alla prevenzione piuttosto che alla cura dei problemi a posteriori.

Le sorgenti di rischio, qui di seguito utilizzate, sono ufficiali poiché provengono da:

- Minacce ENISA
- NIST Risk Management Framework

I pericoli sottesi alle sorgenti di rischio considerate sono seri e in grado di produrre danni rilevanti in termini di funzionalità dei sistemi e di riservatezza delle informazioni.

Articolazione del Regolamento

Il presente Regolamento prevede una prima parte introduttiva dove sono identificate e definite le componenti del sistema di gestione nel suo complesso, a cui segue un elenco che riepiloga per ogni tipologia di servizio o di sistema le corrette modalità di utilizzo.

Infine, sono riportati in appendice alcuni validi strumenti atti a ridurre gli errori tipici degli utilizzatori.

CAPO I - Disposizioni generali

Art. 1. - Oggetto e finalità

1) ASUR Marche è da anni fortemente impegnata in importanti investimenti in tecnologie e servizi dell'informazione per supportare le funzioni di prevenzione, diagnosi, cura e riabilitazione, unite alle attività amministrative e di gestione dei servizi.
   Il presente Regolamento definisce il modello comportamentale considerato accettabile, per gli utilizzatori dei servizi e dei sistemi informatici dell'organizzazione.
2) Al fine di preservare il patrimonio informativo dell'organizzazione, la continuità operativa dei servizi e parallelamente ridurre i rischi di esposizione, sia dal punto di vista sanzionatorio che risarcitorio (tenuto conto delle normative nazionali ed europee vigenti come il GDPR), ASUR Marche richiede agli utilizzatori dei servizi e dei sistemi informatici di conformarsi obbligatoriamente ai dettami del presente Regolamento.

Art. 2. - Ambito di applicazione - Perimetro

1) Il presente Regolamento si applica a tutti gli utilizzatori dei sistemi e dei servizi IT dell'organizzazione compresi nel perimetro, corrispondente alla massima estensione della rete di comunicazione privata fino al firewall di connessione con la rete pubblica, includendo anche i sistemi collegati via Virtual Private Network (VPN) e i sistemi posizionati in zone demilitarizzate (DMZ), in *colocation*, in *hosting*, in *housing* o in cloud.
2) Sono compresi tutti gli elementi della catena tecnologica come le *facility*, il network, i sistemi server, il *middleware*, le applicazioni come anche i sistemi di gestione della sicurezza, il monitoraggio e il controllo, i dispositivi client come i personal computer, i *thin client*, le stampanti multifunzione, i centralini telefonici, i telefoni basati su tecnologia IP, gli smartphone e i tablet.
3) Sono escluse dal perimetro tutte le reti Wi-Fi di tipo *guest* (ad accesso gratuito per il pubblico).
4) Gli utilizzatori dei servizi pubblicati e accessibili da Internet sono esclusi dal perimetro se collegati attraverso connessioni esterne al perimetro (ad esempio sono esclusi coloro che visitano i siti web istituzionali, la sezione relativa agli obblighi di amministrazione trasparente, la consultazione dei referti e degli esami diagnostici online).

Art. 3. - Applicazione del Regolamento IT

1) Gli utenti sono obbligati ad accettare e a conformarsi al presente Regolamento come condizione necessaria per l'accesso e l'utilizzo dei servizi e dei sistemi IT.
2) Il rispetto delle prescrizioni è il prerequisito per un impiego legittimo e ottimale dei servizi e dei sistemi IT, sia per il personale deputato alla gestione che per tutti gli utilizzatori.

Art. 4. - Definizioni

Ai fini del presente regolamento s'intende per:

1) **Minaccia**: qualcosa di potenzialmente pericoloso; possibile evento non desiderato che porta alla perdita di riservatezza, integrità o disponibilità delle informazioni;
2) **Vulnerabilità**: caratteristica dei sistemi e dei processi che identifica una fragilità, un punto debole che in particolari condizioni, può comportare la perdita di riservatezza, integrità o disponibilità delle informazioni;
3) **Contromisure:** azioni di prevenzione e mitigazione delle vulnerabilità individuate al fine di limitare i rischi di perdita di riservatezza, integrità o disponibilità delle informazioni;
4) **Rischio:** probabilità che un evento si verifichi ovvero che una minaccia si trasformi in evento indesiderato e dannoso sfruttando una vulnerabilità;
5) **Fonte di rischio:** elemento tangibile o intangibile che possiede il potenziale intrinseco di originare il rischio singolarmente o in combinazione con altri elementi;

6) **Evento sfavorevole:** particolare insieme di circostanze in grado di modificare in modo negativo e contrario rispetto al normale comportamento di un sistema, ambiente, processo, flusso di lavoro o di una persona;
7) **Conseguenza:** Effetto diretto o indiretto di un evento;
8) **Incidente alla sicurezza:** Evento volontario o involontario attribuibile a una o più persone con associato un costo economico diretto (es. sostituzione del bene e interruzione del servizio) oppure indiretto (uso non autorizzato di informazioni, violazioni di legge, danni di immagine e reputazionali) che comporta una minaccia alla sicurezza;
9) **Impatto (negativo):** Stima delle potenziali perdite dirette o indirette associate a un rischio;
10) **Credenziali di autenticazione:** codice per l'identificazione dell'utilizzatore di un sistema o di un dispositivo associato a una parola chiave riservata, conosciuta solamente dal soggetto (spesso identificata come coppia login o codice utente e password);
11) **Spam:** ovvero spazzatura spesso associata alla posta elettronica (in inglese *junk e-mail*) che indica la ricezione di messaggi spesso indesiderati, ripetuti o monotematici (es. pubblicità) il cui mittente speso è sconosciuto.

Art. 5. - Principi

1) I principi ispiratori del presente regolamento sono:
   a) Tutela dei diritti, delle libertà e della dignità delle persone;
   b) Garanzia della necessaria *continuità operativa* per la miglior cura possibile dei pazienti e il minor dispendio di energie (umane, tecnologiche, temporali ed economiche);
   c) Tutela del patrimonio informativo aziendale e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:
      i. Accessi illegittimi ai sistemi o agli applicativi;
      ii. Modifiche indesiderate alle informazioni;
      iii. Perdita della disponibilità dei dati;
   d) Conformità normativa e allineamento agli standard di mercato;
   e) Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia;
   f) Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
   g) Adozione della Regola del minimo previlegio rispetto alla finalità (*separation of duties policy*), in ottica di stratificazione dei profili e degli accessi;
   h) Diritto alla disconnessione degli utilizzatori dai sistemi *mobile* al di fuori dell'orario di lavoro.

Art. 6. - Condotta e utilizzo etico dei servizi e dei sistemi IT

2) I sistemi e i servizi IT sono forniti agli utenti per condurre e supportare la missione dell'organizzazione, ovvero a tutte le attività legate agli ambiti sanitari e/o tecnici ed amministrativi.
3) Gli utenti sono responsabili dell'utilizzo dei sistemi e dei servizi IT in modo eticamente corretto, sicuro, legale e conforme al presente regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'organizzazione.
4) L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli account aziendali ricevuti, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio personal computer, applicativo software o piattaforma web aziendale e non.
5) All'utilizzatore di sistemi e servizi IT sono tassativamente vietate le seguenti attività:

a. La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
b. La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;
c. La trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri o non omologati dai Sistemi Informativi Aziendali;
d. L'invio di dati di tipo sensibili su canali non sicuri (un esempio di strumento da evitare per inviare dati sensibili è la posta elettronica aziendale, che viaggia in chiaro quando inviata ad altro dominio di posta; è da ritenersi invece accettabilmente sicuro l'invio ad altro utente di posta dello stesso dominio. In caso di dubbi è necessario contattare i Sistemi Informativi Aziendali o adottare tecniche di criptazione con invio della chiave su altro media);
e. La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'organizzazione;
f. L'accesso non autorizzato ai sistemi o ai servizi IT.

6) Gli utilizzatori di sistemi e servizi IT non sono autorizzati a rispondere a interviste telefoniche o sondaggi, compilare questionari on-line (anche se sollecitati da importanti *brand*).
7) L'introduzione degli strumenti mobile (forniti dall'organizzazione o BYOD) pone il problema dell'equilibrio tra vita privata e vita professionale, data la progressiva trasformazione degli strumenti di comunicazione da asincroni a tempo reale. È riconosciuto all'utilizzatore il diritto alla disconnessione[1] dai dispositivi *mobile* al di fuori dell'orario di lavoro e dai turni di pronta disponibilità.
8) Anche nel caso dei sistemi di *instant messaging* (es. WhatsApp) vale il diritto alla disconnessione; è demandato alla sensibilità dei singoli il rispetto della distinzione tra tempistiche professionali e momenti da dedicare alla vita privata e familiare.

Art. 7. - Tipologie di minacce

1) Una prima classificazione delle minacce è riconducibile alla sorgente di produzione:
   - Deliberata o Intenzionale;
   - Accidentale, come perdite involontarie di informazioni o risorse IT;
   - Naturale.
2) In funzione delle tipologie di minacce è necessario attivare tutte le opzioni possibili al fine di ridurre la superficie di esposizione; l'organizzazione e la relativa profilazione dell'utenza è uno dei possibili elementi di attenuazione per quanto riguarda gli attacchi deliberati, mentre per gli eventi accidentali o legati all'inconsapevolezza dei comportamenti a rischio degli operatori è fondamentale un'azione prima di tutto culturale, volta alla sensibilizzazione al tema della sicurezza delle informazioni trattate. Per quanto attiene alle minacce naturali è invece necessario agire sulle infrastrutture e sulla catena tecnologica con adeguati elementi di ridondanza.

Art. 8. - Sistema di gestione della sicurezza dell'informazione

1) Un Sistema di gestione della sicurezza dell'informazione (SGSI o ISMS secondo la norma ISO 27001), è un insieme di politiche e procedure per la gestione sistematica delle informazioni trattate dall'organizzazione. L'obiettivo di un SGSI è ridurre al minimo i rischi e garantire la continuità

[1] L'articolo L. 2242-8 del Codice del lavoro francese ("*Code du travail*") modificato dalla legge Loi n° 2016-1088 (*relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels)* dispone "Le modalità di esercizio da parte del dipendente del proprio diritto alla disconnessione nonché la messa a disposizione di dispositivi che regolano l'utilizzo degli strumenti informatici, al fine di assicurare il rispetto dei tempi di riposo, del periodo di ferie e della vita personale e familiare". In Italia esiste al momento solo un disegno di legge n. 2233 su lavoro autonomo.

aziendale agendo sugli aspetti di sicurezza logica, fisica ed organizzativa, al fine di limitare proattivamente l'eventuale impatto di una violazione.

2) Il presente regolamento come anche le procedure, la modulistica e le linee guida, sono parte integrante del SGSI.

CAPO II - Strumenti

Art. 9. - Identificazione, autenticazione e autorizzazione

1) L'organizzazione implementa nella gestione dei sistemi e dei servizi IT, la famiglia di protocolli AAA basata sulle funzioni di Autenticazione, Autorizzazione, Accounting (v. articolo successivo).
2) Quanto previsto in questa sezione non si applica ai servizi pubblici, che non richiedono autenticazione e ai sistemi ad alta rotazione e intensità (es. Pronto Soccorso) dove sono previsti account di accesso multiutente (cosiddetti account generici) e successivamente sono tracciate le singole attività eseguite a livello di applicazione software (*application log*).
3) L'accesso alla rete e ai sistemi dell'organizzazione è possibile soltanto se l'utilizzatore:
   a) È stato prima di tutto ***identificato*** ovvero sono conosciute le sue generalità ed è stato dotato di credenziali utente (nome utente, password e/o PIN), soggette alle condizioni previste in questa sezione del Regolamento;
   b) Effettua l'***autenticazione*** tramite immissione delle credenziali, in modo che il sistema possa verificare se l'individuo è chi sostiene di essere;
   c) È stato ***autorizzato*** ovvero è stato conferito il diritto ad accedere a specifiche risorse in base al ruolo ricoperto, al profilo e alle specifiche mansioni assegnate.
4) La responsabilità delle azioni effettuate utilizzando la coppia "nome utente e password e/o PIN" sarà attribuita in termini di responsabilità al soggetto titolare dell'account, a meno di comprovato illecito da parte di terzi. Sono escluse le attività di supporto autorizzate dagli stessi utilizzatori per interventi di manutenzione o assistenza tecnica.
5) **Gli account di accesso del personale dipendente, dei consulenti esterni e dei fornitori sono di tipo nominativo e non riutilizzabile da altri soggetti, anche dopo la conclusione del rapporto di lavoro.**
6) Gli account di accesso hanno, per impostazione predefinita, una scadenza corrispondente alla data di fine del contratto, convenzione o accordo. È a carico del Dirigente Responsabile comunicare al personale dei Sistemi Informativi l'eventuale prolungamento del contratto e la necessità di estensione temporale delle autorizzazioni (attività obbligatoria nel caso di mancata copertura da parte del sistema di gestione aziendale delle identità, direttamente integrato con il gestionale HR).
7) Il personale dei Sistemi Informativi specificatamente autorizzato gestisce gli account utente per tutto il ciclo di vita tramite apposita procedura (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, disattivazione una volta concluso il rapporto di lavoro).
8) La normativa vigente in tema di protezione dei dati, le norme volontarie e le *best practice* di settore impongono di stratificare le possibilità di accesso ai sistemi e ai servizi IT al fine di garantire un adeguato livello di sicurezza. Ad ogni account utente è collegato uno specifico *profilo di autorizzazione* che permette al singolo utilizzatore l'accesso in funzione del proprio ruolo, delle attività a cui è delegato e specificatamente autorizzato da un superiore (o soggetto Designato ai sensi del D.lgs. 196/03 e ss.mm.ii.). Le eventuali estensioni o eccezioni devono essere autorizzate e tracciate secondo procedura.
9) Il sistema di Autenticazione, Autorizzazione e Registrazione degli accessi ha l'obiettivo di garantire un adeguato livello di sicurezza, conforme a quanto previsto dalla normativa vigente e dal presente regolamento, poiché traccia, separa gli accessi nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni trattate.

Art. 10. - Registrazione delle attività (*Accounting*)

1) A partire dall'accesso ai sistemi o ai dispositivi, le attività degli utilizzatori sono registrate in appositi file detti di *log*. Nei sistemi critici, di particolare rilevanza o di fede privilegiata sono memorizzate tutte le singole attività svolte riportando utente, indirizzo o nome macchina, ora, data e il dettaglio delle azioni svolte.
2) Al fine di contenere lo spazio necessario alla conservazione, i file di log sono conservati in logica di rotazione, ovvero sono sovrascritti al raggiungimento di una certa data o di una certa dimensione.
3) Alcuni file di log (es. log di accesso) sono conservati nei sistemi per almeno 2 anni dall'evento.

Art. 11. - Corretto uso delle Credenziali di autenticazione

1) Le credenziali di autenticazione sono composte da un codice (account utente) facilmente riconducibile al soggetto e da una *password e/o PIN conosciuti al solo utilizzatore*. ***È tassativamente vietato rivelare la propria password*** di accesso alla rete, agli applicativi o servizi disponibili (inclusi i siti regionali o ministeriali). Qualsiasi azione effettuata utilizzando la coppia "account utente e password e/o PIN" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.
2) Gli account di accesso dell'organizzazione non devono essere utilizzati per la registrazione o autenticazione federata a sistemi o siti web che non siano istituzionali di livello regionale o nazionale. Eventuali eccezioni devono essere autorizzate dai Sistemi Informativi Aziendali.
3) La *lunghezza minima della password* deve essere di almeno 8 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri[2] per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e per gli account qualificati amministrazione di sistema.
4) Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione (es. Mi_P1@c3_l4_P1zz@).
5) È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. L'eventuale violazione di un sistema potrebbe comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, aziendali e personali riconducibili allo stesso soggetto.
6) Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 3 mesi (cd. *Password aging*).
7) Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, oppure essere troppo ovvie (es. 'P@ssword').
8) Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (il precedente elenco non è esaustivo).
9) Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (criteri di complessità).
10) Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. *Password history*);
11) Le password degli account di accesso ai sistemi non sottoposti alle politiche di complessità, di invecchiamento o di rotazione impostate nel sistema di autenticazione centrale, devono comunque rispettare le medesime regole, agendo manualmente.

[2] Misura minima prevista da AgID - «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017)

12) Le password e i PIN non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso o primo invio). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.
13) La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti.
14) I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.
15) È vietata la memorizzazione delle password nei browser o tramite applicativi di gestione password (es. Pocket Password) se non direttamente autorizzati/distribuiti dal SIA (nel caso si utilizzi Mozilla Firefox è possibile memorizzare le password nel browser solo nel caso di attivazione della funzione 'Utilizza una password principale' inserendo una password estremamente complessa e lunga). Sono comunque esclusi sistemi o applicativi software di memorizzazione delle credenziali nel cloud.
16) Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile al solo fine di verificarne la robustezza; es. https://password.kaspersky.com/it).
17) Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).
18) Non seguire le mode del momento, utilizzare acronimi, pattern ('CristianoRonaldo$' oppure sempre il primo carattere di ogni parola maiuscolo e un dollaro finale), ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari (in Appendice 1 - Password presenti nei dizionari pubblici sono riportate degli esempi di password da NON utilizzare).
19) Nel caso di perdita (o anche solo il sospetto di perdita) della segretezza della password è necessario:
    a. Modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e Cambia password; verificare le modalità per i singoli applicativi con autenticazione locale);
    b. Comunicare l'accaduto ai Sistemi Informativi Aziendali, al proprio Responsabile e al DPO per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure del caso.
20) Nel caso l'utilizzatore sbagli per più di 5 volte l'inserimento della password, l'account è automaticamente disabilitato; per effettuare la riabilitazione dell'account è necessario contattare il supporto tecnico, aprire un ticket o, se presente, utilizzare il sistema di *selfservice password*.
21) In caso di prolungato inutilizzo dell'account (per più di 6 mesi), in caso di cessazione o trasferimento degli utilizzatori, il sistema di Gestione delle Identità provvede all'automatica disabilitazione. L'eventuale riabilitazione dovrà essere autorizzata da un superiore soggetto Designato.
22) Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, il SIA è autorizzato alla momentanea disattivazione dell'account e del sistema utilizzato. Risolta la problematica evidenziata sarà cura del SIA ripristinare le precedenti autorizzazioni.
23) Le richieste di cambiamento o reset password dell'account di accesso ai sistemi dell'organizzazione non sono mai inviate tramite e-mail. Eventuali e-mail che richiedano tramite link la modifica della password devono essere marcate come spam e cestinate.
24) È tassativamente vietato memorizzare account di accesso ai sistemi e servizi aziendali in documenti salvati in sistemi o dispositivi al di fuori del perimetro aziendale e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive o Dropbox).
25) Gli account di amministrazione di dominio possono essere utilizzati soltanto nei client assegnati al personale dei Sistemi Informativi o posizionati nel data center; questo al fine di evitare problemi di registrazione delle password attraverso *keylogger* hardware o software.

26) I fornitori di sistemi e servizi IT sono obbligati a impostare la funzione di reset password self-service (che permette la re-impostazione della password senza necessità di chiamata al supporto tecnico) che in caso di momentanea dimenticanza velocizza le operazioni di ripristino ed evita inutili sovraccarichi al servizio tecnico.

Art. 12. - Posta elettronica convenzionale

1) La posta elettronica è uno strumento di comunicazione aziendale e deve essere utilizzato soltanto per effettuare corrispondenze legate al servizio svolto nell'organizzazione.
2) Ogni utilizzo della posta elettronica deve essere effettuato coerentemente con le politiche e le procedure dell'organizzazione nel rispetto dell'etica, della sicurezza e in piena conformità alle leggi applicabili.
3) La posta elettronica non deve essere utilizzata per la creazione, distribuzione o rilancio di messaggi di disturbo o offensivi, commenti su l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, lo stato di salute o la disabilità, il genere, il colore dei capelli, l'età, la vita o l'orientamento sessuale della persona. I dipendenti che dovessero ricevere messaggi con queste tipologie di contenuto da qualsiasi dipendente, devono segnalare immediatamente la questione al diretto superiore.
4) La posta elettronica non deve essere utilizzata per inviare messaggi massivi ad una moltitudine di utenti, in particolare per diffondere locandine, inviti o pubblicizzare eventi, prediligendo la pubblicazione sul sito intranet aziendale nella sezione *news* o eventi, a meno di informazioni particolarmente importanti o urgenti, e comunque su specifica autorizzazione della Direzione Generale o di Area Vasta.
5) La posta elettronica ordinaria o e-mail secondo la recente giurisprudenza[3], rispetto a quanto previsto dal Regolamento (UE) 2014/910 eIDAS (*electronic IDentification Authentication and Signature*) e dalle conseguenti modifiche al D.lgs. n. 82/2005 CAD (Codice dell'Amministrazione Digitale) ha validità giuridica e rilevanza probatoria[4], è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
6) Un messaggio di posta elettronica convenzionale inviato allo stesso dominio (@sanita.marche.it) ha un livello di sicurezza mediamente elevato; nel caso di invio ad altri domini anche se istituzionali (ministeri, regioni, comuni, ecc.) il livello di sicurezza potrebbe essere equiparabile alla semplice cartolina postale. Per questo motivo è necessario verificare il destinatario, soprattutto se multiplo, e in particolare il contenuto della comunicazione (testo e allegati).
7) Alla fine della sessione di lavoro è necessario effettuare sempre la disconnessione (Log out) dal sistema di posta, client locale o web.
8) L'indirizzo di posta elettronica non deve essere utilizzato per la registrazione a siti che non siano in qualche modo legati alle attività svolte dagli utilizzatori intestatari nell'organizzazione, anche al fine di limitare lo spam.
9) Non lanciare mai i link di annullamento alle sottoscrizioni delle e-mail considerate indesiderate (il cd. "*unsubscribe*"), al fine di ridurre il rischio di conferma dell'esistenza e utilizzo della e-mail.
10) Al fine di garantire la corretta coerenza comunicativa dell'organizzazione, è vietato modificare il *footer* (parte finale del messaggio) rispetto allo standard dell'organizzazione.
11) I sistemi di sicurezza come firewall e antispam garantiscono con discreta probabilità che le e-mail consegnate siano esenti da pericoli. È sempre a carico dell'utilizzatore la verifica ultima di:

[3] Sentenze n. 14716/2011 e n. 11402/2016 Tribunale di Milano

[4] Dalla definizione CAD di "firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica", l'utilizzo delle credenziali di accesso alla casella di posta elettronica vale a qualificare l'utente e costituisce pertanto una firma elettronica semplice, non avanzata né qualificata, ma comunque non giuridicamente irrilevante e sotto il profilo probatorio liberamente valutabile in giudizio

a. **Mittente**: deve essere conosciuto (da verificare l'indirizzo effettivo e non la semplice denominazione); esempio da evitare e marcare come spam è il mittente service145@mail.145.com;
b. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo *phishing*; la verifica può essere fatta posizionando il cursore del mouse sul link per visualizzare la reale destinazione (ad esempio evitare di fare click su link del tipo http://amazon.net.ru);
c. **Allegati**: diffidate dei file con estensione multipla o senza estensione o con denominazione estranea alle attività o mansioni svolte abitualmente (es. 'Si allega fattura');
d. **Contenuti**: scrittura con errori grossolani (traduzione da sistemi automatici), riferimenti alla chiusura di un conto o di un servizio, parole come URGENTE, richieste di dati personali o di password, file che non sono mai stati richiesti o con estensioni sospette.

12) Nei casi dubbi non aprire le e-mail o i contenuti e contattare il supporto tecnico che provvederà alla verifica secondo le procedure di sicurezza.
13) È vietato il *forward* o rilancio della posta sui dispositivi mobili (es. smartphone e tablet) personali. Il *forward* dei messaggi è permesso solamente sui dispositivi mobili di proprietà dell'organizzazione, agli utilizzatori specificatamente autorizzati.
14) L'utilizzo di *forward* di posta automatico dell'organizzazione su altri sistemi (es. Gmail) è vietato; questo al fine di garantire un adeguato livello di sicurezza dei contenuti dei messaggi come ad esempio gli allegati contenenti dati personali o riservati inviati dal mittente che, non essendo a conoscenza del rilancio, non adotta le misure necessarie alla protezione dei contenuti prevista per trasferimenti al di fuori dell'Unione Europea.
15) La posta elettronica fornita dall'organizzazione non può essere utilizzata per scopi personali estranei all'attività lavorativa. Viceversa, è vietato utilizzare o fornire e-mail personali per scambiare informazioni, contenuti o allegati legate all'attività lavorativa.
16) L'invio di file tramite link ai sistemi di hosting è permesso solo se i file sono criptati e le chiavi di criptazione sono condivise su altro media. Le procedure di criptazione sono disponibili nella intranet istituzionale.
17) Non consultare la posta elettronica dell'organizzazione presso Internet point, Wi-Fi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar).
18) Le raccomandazioni o indicazioni inviate via e-mail non devono essere seguite poiché nella maggior parte dei casi si tratta di virus HOAX (cd. bufale). In caso di dubbi contattare il supporto tecnico SIA.
19) Marcare come spam le e-mail che appaiono come *scam* ovvero tentativi di truffa pianificata con metodi di ingegneria sociale (in genere nella e-mail si promettono enormi guadagni in cambio di somme di denaro da anticipare).
20) Le e-mail che richiedono l'attivazione delle macro di MS-Word o MS-Excel prima del download degli allegati devono essere immediatamente marcate come spam.
21) Non attivare mai i link presenti nelle cosiddette e-mail di reset della password.
22) Non rispondere e inoltrare e-mail delle cosiddette catene di Sant'Antonio o rispondere alle e-mail di spam.
23) La policy della posta elettronica prevedono le seguenti limitazioni:
    a. Dimensione massima della casella di posta elettronica è paria 2.5 GB (evitare di trasformare il sistema di posta elettronica in sistema di archiviazione), mentre è pari a 500 MB per gli utenti base;
    b. Dopo 14 mesi, la posta viene spostata automaticamente in un archivio on line;
    c. Dimensione massima degli allegati inviati o ricevuti pari a 10 MB;
    d. Limite massimo di destinatari contemporanei pari a 100;
    e. Limite delle *Address list* creabili pari a 1000;

f. Limite del *forwarding* pari a 10 recipienti;

24) Gli allegati inviati via e-mail contenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste in questi casi. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (es. via telefono).
25) Le e-mail contenenti evidenze di reati penali devono essere prima visionate dal personale tecnico del SIA e poi, se del caso, informate le autorità per la presentazione della denuncia; questo al fine di evitare falsi allarmi.
26) Al fine di ridurre il traffico e soprattutto il rumore nelle comunicazioni, i mittenti delle e-mail devono seguire le regole previste nella seguente matrice:

Livello gerarchico	Comparto stessa UO	Comparto altre UO	Direttore UOS/UOC	Altri Dirigenti di UO	Direzione generale
Comparto	Secondo le necessità di servizio	Secondo le necessità di servizio	Solo se necessaria autorizzazione o per conoscenza	Solo in caso di emergenza o di escalation	Solo in caso di emergenza
Direttore UOS/UOC	Secondo le necessità di servizio	Solo se in conoscenza al Direttore UOS/UOC	-	Secondo le necessità di servizio	Secondo le necessità di servizio
Direzione generale	Solo in caso di emergenza	Solo in caso di emergenza	Secondo le necessità di servizio	Secondo le necessità di servizio	-

27) In casi particolari, di emergenza o semplicemente nel caso non si ricevano le risposte nei tempi attesi, è possibile effettuare la cosiddetta *escalation* ovvero scrivere direttamente al diretto superiore del primo destinatario. Le comunicazioni in modalità *escalation*, se considerate inutili, espongono il mittente alle sanzioni disciplinari previste.
28) L'utilizzatore del sistema di posta, in caso di sospensione del servizio per ferie o malattia, è tenuto autonomamente all'impostazione del messaggio di risposta automatica delle e-mail e alla richiesta di inoltro ai colleghi oppure al diretto superiore.
29) L'invio di dati particolari tramite posta elettronica convenzionale è permesso soltanto nel caso il file sia criptato secondo la procedura prevista (punto 24).
30) In caso di assenza dell'utilizzatore intestatario dell'account e-mail e in presenza di specifiche necessità istituzionali di accesso ai messaggi di posta, il diretto superiore può richiedere ai Sistemi Informativi l'accesso al singolo messaggio o all'intera cartella, il *forward* momentaneo o definitivo della posta su altro indirizzo. Di tale attività deve essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.
31) Nel caso si riceva una e-mail visibilmente contraffatta da un collega, è necessario informare immediatamente il supporto tecnico.
32) Nel caso la marcatura come messaggio indesiderato di un insieme ricorrente di messaggi di spam non riduca il problema, è possibile attivare i cosiddetti filtri personalizzati, in grado di marcare automaticamente tipologie di e-mail indesiderate; nella Intranet sono disponibili le istruzioni per l'attivazione della funzionalità.
33) Al fine di contenere lo spazio di memoria del server di posta è necessario conservare solo e-mail rilevanti per la propria attività. Le e-mail non più utili devono essere eliminate (soprattutto se con allegati di dimensioni elevate).
34) L'utente deve organizzare la propria casella di posta in modo tale che ci sia una separazione tra l'archivio corrente e quello storico secondo la regola:

Archivio on line
Posta in Arrivo – 2018

2019
2020

I dati meno recenti potranno così essere memorizzati in modo automatico in contenitori a prestazioni meno elevate.

35) Nel caso di comportamenti anomali del personal computer evidenziati a seguito dell'apertura di una e-mail, di un click su un link o di un download di un file, è necessario:
    a. Staccare immediatamente il cavo di rete;
    b. Spegnere il computer;
    c. Segnalare immediatamente l'accaduto al SIA e al proprio Dirigente.

Art. 13. - Posta Elettronica Certificata (PEC)

1) La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, ed è garantita la tracciabilità della casella mittente; il circuito è certamente più sicuro della posta elettronica convenzionale ma non è esente da rischi. Per questo motivo valgono le stesse regole e indicazioni fornite per la posta elettronica convenzionale.
2) L'invio tramite PEC di documentazione riservata o contenente dati personali particolari deve avvenire sempre attraverso allegati criptati con comunicazione delle chiavi attraverso altro media. Da notare che molte PEC di enti pubblici sono direttamente collegate con i sistemi di protocollazione e archiviazione sostitutiva, accessibili a personale seppur deputato allo smistamento ma con livelli di autorizzazioni non elevati e soprattutto non è prevedibile a priori né le modalità di smistamento, né i profili che potranno accedere alle informazioni inviate. Da verificare quindi la necessità/possibilità di protocollazione degli allegati, specie se criptati.

Art. 14. - Firma elettronica

1) Le Firme Elettroniche, ai sensi del Regolamento UE n. 910/2014 (eIDAS, *Electronic IDentification Authentication and Signature*) e del CAD possono essere di 4 tipi:

Tipologia Firma	Definizione	Esempi	Valore probatorio
Elettronica semplice [art. 3, comma 10 eIDAS]	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare	Messaggio di posta elettronica ordinaria o una sottoscrizione (scansione firma apposta al documento) che non ha tutti i requisiti delle altre sottoscrizioni elettroniche di livello superiore	Liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21 del CAD)
Avanzata [art. 3, comma 11 eIDAS] [Requisiti previsti all'art 26 eIDAS]	a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.	Firma grafometrica utilizzata su tablet in molti contesti tra i quali le banche e le assicurazioni.	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
Qualificata [art. 3, comma 12 eIDAS]	Firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche	Smart card, Token (sicurezza)	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma

			qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
Digitale [art. 24 CAD]	Particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Smart card, Token (sicurezza), Firma digitale remota.	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

2) L'utilizzatore dotato di strumenti di firma è responsabile della conservazione in sicurezza di tutte le componenti (hardware come la Smart card, PIN e Password). La perdita degli strumenti di firma o il semplice sospetto della perdita di segretezza della password o del PIN, deve essere immediatamente comunicata al supporto tecnico SIA e al DPO.
3) È fondamentale conservare separati i dispositivi di firma (Smart card) dal PIN e dalla password (è preferibile provare a ricordare, senza dover trascrivere le credenziali).
4) La firma di atti o documenti dell'organizzazione è responsabilità diretta dell'intestatario della firma elettronica (di qualsiasi tipologia sopra riportata). È vietato firmare per conto di altri soggetti anche nel caso di autorizzazione verbale o scritta; sono escluse dal divieto le sole firme cosiddette automatiche (es. attraverso il sistema SDI).
5) I documenti firmati digitalmente, per definizione, non sono ripudiabili a meno di querela di parte.
6) È possibile firmare atti o documenti dell'organizzazione solo se in formato PDF, PDF/A (progettato per la conservazione dei documenti amministrativi) o XML. Gli altri formati sono vietati, a meno di specifica autorizzazione.
7) Le tipologie di firme accettate sono P7M (CAeDES) e PDF (PAeDES). Altri formati non sono accettati dall'organizzazione o dalle piattaforme di conservazione.
8) Il rinnovo dei certificati di prossima scadenza è in carico a Regione Marche o di altri fornitori del servizio di firma. L'aggiornamento dei certificati del software di verifica delle firme è a carico del singolo utilizzatore. Contattare il supporto tecnico SIA nel caso di problemi.
9) Le regole per la sicurezza delle password riportate all'Art. 11. - del presente regolamento sono valide anche nella definizione della password e PIN/PUK di firma.
10) Nel caso il software di verifica delle firme segnali delle anomalie è necessario:
    a. Verificare che la lista delle *Certification Authority* (CA) sia aggiornata;
    b. Verificare il firmatario;
    c. Eventualmente richiedere di nuovo il documento firmato al firmatario.
11) La conservazione sostitutiva dei documenti firmati digitalmente segue quanto previsto dalla regolamentazione in materia. Si faccia riferimento alla specifica documentazione a cura del Responsabile della conservazione e della transizione digitale.
12) La documentazione firmata deve seguire un percorso di archiviazione in base al Regolamento aziendale in materia, a cura del responsabile della conservazione.

Art. 15. - Instant messaging

1) Gli strumenti di comunicazione sincrona permettono facili e immediati scambi di messaggi di servizio tra colleghi; permettono anche la condivisione dei documenti, delle immagini e dei video senza richiedere particolari prerequisiti a meno della copertura Internet o Wi-Fi e l'utilizzo di un dispositivo *mobile*. I prodotti più diffusi sono WeChat, Facebook Messenger e WhatsApp. L'utilizzo

di questi strumenti in ambito lavorativo è tollerato per le sole comunicazioni interpersonali di servizio (appuntamenti, segnalazioni urgenze, ecc.).

2) La condivisione di dati personali o di informazioni riservate relative all'ambito lavorativo su piattaforme di messaggistica è vietato per le seguenti motivazioni:
    a. I dati sono inviati (inconsapevolmente) in server posizionati in paesi Extra UE, senza le dovute prescrizioni previste al Capo V del GDPR, artt. 44-50 in termini di regolamentazione, protezione e garanzie per gli interessati;
    b. Tutte le informazioni (testo, immagini e video) sono indicizzate per denominazione e contenuti;
    c. Tutti gli utenti sono profilati anche se non appartenenti allo specifico ambito o sconosciuti al sistema;
    d. Non è al momento prevedibile quale utilizzo sarà fatto in futuro dei dati inviati, né quali potranno essere gli impatti sugli interessati;
    e. I backup di WhatsApp (famiglia Facebook) su dispositivi basati su Android sono, al momento, salvati direttamente su Google Drive in modalità non criptata, il che permette al secondo big dell'indicizzazione di accedere ad ulteriori informazioni;
    f. Le impostazioni di sicurezza dei dispositivi *mobile* generalmente non garantiscono un adeguato livello di protezione dei dati.
3) Eventuali messaggi arrivati su dispositivi *mobile* contenenti dati personali o informazioni riservate legate all'ambito lavorativo devono essere cancellate.
4) Le APP per *mobile* possono essere scaricate soltanto dagli *store* ufficiali. In caso di dubbi sugli strumenti aziendali in uso contattare il supporto tecnico.
5) Verificare periodicamente le impostazioni relative alle autorizzazioni delle applicazioni dei dispositivi *mobile* e le relative impostazioni sulla privacy.
   Per i sistemi di messaggistica istantanea valgono le stesse considerazioni di sicurezza esposte nei commi relativi alla posta elettronica, in particolare per quanto riguarda mittenti, contenuti, link e allegati.

Art. 16. - Dispositivi Mobili (smartphone, tablet e *pen drive*/*portable disk*)

1) L'uso personale dei dispositivi mobili forniti dall'organizzazione è tollerato a patto che non siano salvati nel sistema dati personali estranei all'attività lavorativa. Eventuali documenti contenenti dati personali devono essere rimossi immediatamente.
2) È vietata l'installazione di applicazioni non direttamente distribuite, autorizzate e presenti nella *white list* dell'organizzazione, anche se provenienti dagli *store* ufficiali.
3) I dispositivi *mobile* forniti dall'organizzazione hanno impostazioni di sicurezza predefinite, conformi alla normativa vigente e alle policy aziendali. È vietato modificare le impostazioni di sicurezza anche se al fine di permettere il funzionamento di applicazioni software, se non specificatamente omologate dai Sistemi Informativi Aziendali. Contattare il supporto tecnico in caso di problemi.
4) Nell'ipotesi di smarrimento o furto di un dispositivo fornito dall'organizzazione e contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, l'utilizzatore è tenuto a comunicare l'accaduto al DPO/RPD per l'attivazione della procedura di data *breach* e, a seguire, ai Sistemi Informativi Aziendali per l'attivazione delle previste procedure di sicurezza (*device wipe-out*).
5) Il trasporto al di fuori del perimetro aziendale di dispositivi di memorizzazione aziendali contenenti dati sensibili è vietato. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori del perimetro aziendale, sarà attribuita all'utilizzatore assegnatario.
6) In tutti i casi di trasporto dei dati al di fuori del perimetro della rete aziendale è tassativamente prevista la criptazione dei contenuti, anche nel caso di pseudonimizzazione.

7) I commi precedenti non si applicano ai dati totalmente anonimizzati.

Art. 17. - BYOD (*bring-your-own-device*) - Dispositivi di proprietà personale

1) I cosiddetti BYOD (*Bring Your Own Device*, letteralmente "porta il tuo dispositivo") possono essere utilizzati soltanto come sistemi isolati non collegati alla rete dell'organizzazione, a meno del Wi-Fi con accesso di tipo *guest* (se presente). I sistemi di monitoraggio effettuano controlli automatici continui e segnalano al personale del SIA i sistemi e i dispositivi non catalogati e non autorizzati che abbiano effettuato un collegamento diretto alla rete locale aziendale (LAN). Eventuali sistemi o dispositivi non autorizzati collegati alla rete dell'organizzazione saranno bloccati e considerati come attacco al sistema informatico, segnalati alla Polizia Postale e delle Comunicazioni per la denuncia di reato di accesso abusivo a sistema informatico ai sensi dell'Art. 615/ter del Codice Penale.
2) È severamente vietato il collegamento alla rete dell'organizzazione di sistemi o dispositivi non distribuiti ufficialmente dal SIA o dall'Ingegneria Clinica. Il personale che effettuerà il collegamento diretto alla rete dell'organizzazione (sono escluse i Wi-Fi pubblici) sarà soggetto a sanzioni disciplinari. Saranno inoltre addebitati all'utilizzatore eventuali costi di rispristino o ulteriori danni che dovessero originarsi da un collegamento non autorizzato.
3) Il collegamento alla rete Wi-Fi pubblica dell'organizzazione (ove disponibile) dei dispositivi di proprietà personale come laptop, tablet o smartphone è possibile seguendo la specifica procedura di autorizzazione, registrazione e autenticazione.
4) In conformità alla normativa vigente in tema di protezione dei dati personali è vietato salvare sui BYOD i dati personali, specialmente se di natura particolare, raccolti durante le attività lavorative.
5) Il trasporto al di fuori del perimetro aziendale di dispositivi di memorizzazione personali contenenti dati sensibili è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
6) Nell'ipotesi di smarrimento o furto di un dispositivo BYOD contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, è obbligatorio comunicare l'accaduto al DPO/RPD per l'attivazione della procedura di *Data Breach.*

Art. 18. - Navigazione Internet

1) Internet è la fonte di informazioni e documentazione più vasta esistente, quindi irrinunciabile tanto per il personale sanitario quanto per il personale amministrativo. L'interoperabilità tra enti pubblici passa sia attraverso il Sistema Pubblico di Connettività sia attraverso la rete Internet, con una serie di servizi indispensabili al funzionamento della macchina amministrativa. L'azienda mette a disposizione questo servizio a patto che se ne faccia buon uso ovvero che le finalità di navigazione siano connesse esclusivamente all'attività lavorativa.
2) A meno di specifica autorizzazione del proprio Dirigente comunicata al Dirigente SIA, è vietato navigare in tutti i siti web appartenenti alle categorie previste nell'Appendice *Content Filtering Rating Categories*, navigare per fini ludici o personali, utilizzare i social network, effettuare upload o download di file e documenti non connessi all'attività lavorativa, effettuare streaming audio o video (es. radio o tv via Internet), telefonare (es. Skype), effettuare chat on-line se non specificatamente autorizzati.
3) È tassativamente vietata la navigazione in siti Internet palesemente incompatibili con le finalità aziendali, che istighino a comportamenti illegali, che consentano o siano a rischio di diffusione di virus, cavalli di Troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, *hacking* o pirateria informatica a danno dei computer di altri utenti interni o esterni al perimetro aziendale.

4) È inoltre vietato navigare in siti web che possano comportare nei sistemi deputati al monitoraggio e alla protezione della connessione Internet, trattamenti involontari di dati personali di tipo sensibile riconducibili agli utilizzatori del servizio (esempio convinzioni religiose, politiche, stato di salute, vita sessuale).
5) La navigazione web non è esente da rischi, nonostante siano già attivi diversi strumenti di protezione; gli impatti potrebbero non essere legati al singolo computer ma interessare parte o addirittura l'intero patrimonio informativo aziendale, con risvolti imprevedibili sulla continuità stessa dei servizi e danni reputazionali e di immagine. Per queste motivazioni è sempre in capo al singolo utilizzatore la verifica di:
    a. **Indirizzo del sito web**: è necessario verificare più di una volta l'indirizzo completo (attenzione ai siti web che appaiono simili ma non lo sono: www.sanitammarche.it o www.sanita.marche.<*sitowebstrano*>.it; la dimensione del font della barra dell'indirizzo non aiuta);
    b. **Certificato**: evitare i siti non sicuri (con protocollo http) e nel caso di siti in https fare attenzione alla perfetta corrispondenza del certificato con intestazione e indirizzo del sito web in questione;
    c. **Riferimenti**: i siti dei cosiddetti *scammer* o truffaldini non riportano né l'indirizzo della sede né tantomeno numeri telefonici o altri riferimenti;
    d. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto nell'aspetto grafico); questo al fine di evitare attacchi di tipo *phishing*; la verifica può essere effettuata posizionando il cursore del mouse sul link in modo da visualizzare la destinazione reale (ad esempio evitare di fare click su link del tipo www.regione.marche.it nel caso vi sia un rimando ad altro sito, ad esempio: www.<altrositostrano>.it);
    e. **Download**: evitare di scaricare da siti non ufficiali qualsiasi documento, software applicativo, driver o componente aggiuntivo (*plug-in* del browser o componenti "dinamici" come ActiveX o funzioni JavaScript), includendo anche le app per dispositivi *mobile*;
    f. **Contenuti**: verificare la presenza di errori sintattici grossolani (dovuti a traduzione automatiche) al fine di riconoscere siti non ufficiali (tecnicamente denominati *fake*);
    g. **Verifiche web**: attraverso i motori di ricerca è possibile trovare altre informazioni sul sito che possono aiutare nell'identificazione; provare ad effettuare una ricerca web con la denominazione del sito seguita dalle parole "opinioni" o "recensioni" (su un motore <altrositostrano>.it opinioni).

    Nei casi dubbi non aprire il sito web o interrompere la navigazione, chiudere il browser e, nel caso il sistema inizi ad avere comportamenti singolari, disconnettere il sistema dalla rete locale e contattare immediatamente il supporto tecnico che provvederà ad effettuare le verifiche secondo le procedure di sicurezza.
6) L'utilizzo moderato e sporadico degli strumenti informatici aziendali per finalità private è tollerato, solo nel caso che questo non comporti nocumento all'attività lavorativa.
7) I rischi derivanti dall'utilizzo delle informazioni personali (ad es. numeri di carte di credito) durante la navigazione web estranea alle attività lavorative, sono sempre in capo all'utilizzatore. ASUR Marche non potrà essere ritenuta responsabile di eventuali danni dovuti a perdite di riservatezza, integrità o disponibilità di dati personali inviati in sessioni effettuate con strumenti aziendali e in orario di lavoro.
8) L'acquisizione, conservazione, trasmissione o diffusione di file dal contenuto illegale, discriminatorio per origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, o appartenenza sindacale, stato di salute o disabilità, genere, colore dei capelli, età, vita sessuale o orientamento sessuale della persona è vietato. Eventuali abusi o contenuti illegali che si dovessero

evidenziare durante la navigazione devono essere comunicati al supporto tecnico per le valutazioni del caso.

9) L'acquisizione, conservazione, trasmissione o diffusione di materiale che violi il diritto d'autore, i marchi, i segreti commerciali o i diritti di brevetto di qualsiasi persona o organizzazione è vietato. Tutti i materiali pubblicati su Internet sono protetti da copyright e/o brevettati, salvo diversa indicazione[5] (Legge 633/1941 – "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).
10) La trasmissione di informazioni proprietarie, riservate o altrimenti sensibili, contenenti dati personali di tipo particolare è vietata. Solo se specificatamente autorizzato, l'utente può effettuare l'invio/upload a condizioni di adottare controlli specifici e livelli di protezione elevati forniti dalla criptazione.
11) La larghezza di banda della rete locale (interna) dell'organizzazione come anche la connettività Internet è una risorsa condivisa e limitata. Considerato che gli utilizzi indebiti di un singolo utilizzatore potrebbero impattare sulle attività degli altri, sono adottate delle politiche di gestione della banda in funzione delle tipologie di attività svolte che garantiscono il massimo delle prestazioni possibili in funzione delle priorità (*packet shaping*).
12) Le attività di navigazione internet degli utilizzatori sono monitorate da un sistema automatico che verifica i seguenti parametri:
    a. Quantità di dati scaricati giornalmente e mensilmente (inferiore ai 250 Mbyte/giorno);
    b. Tipologie di siti visitati (in vista aggregata e conformi alle politiche di *content filtering*);
    c. Tempistiche totali di navigazione Internet.

    Eventuali comportamenti degli utilizzatori anomali, non conformi o superiori ai parametri generali sopra riportati, quindi non funzionali al corretto funzionamento del servizio, possono comportare la disattivazione automatica dell'account di accesso per motivi di sicurezza o al fine di garantire la necessaria continuità operativa.
13) In conformità alla normativa sulla protezione dei dati personali e perseguendo i principi generali ovvero necessità, correttezza, pertinenza e non eccedenza, è garantita la sovra-registrazione dei dati del traffico Internet dell'utilizzatore, la cui conservazione non sia necessaria (è attivata la cd. rotazione dei log file).
14) La conservazione dei file di registrazione della navigazione degli utilizzatori è limitata a 30 giorni, che è considerato il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, fatti salvi in ogni caso specifici obblighi di legge.

Art. 19. - Utilizzo del personal computer (desktop) o del portatile (laptop)

1) La continuità dei servizi è strettamente legata alla normale operatività di tutti i dispositivi della catena tecnologica, a partire dalla postazione di lavoro. Utilizzi impropri dei dispositivi e delle apparecchiature possono produrre effetti indesiderati e compromettere il funzionamento che, in casi particolari, potrebbe causare danni alle persone. L'utilizzatore di sistemi e servizi IT sarà ritenuto responsabile per i costi di riparazione nel caso che il danno sia causato da uso improprio o da negligenza.
2) È vietato modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete aziendale e all'alimentazione elettrica, da parte dell'utilizzatore o di personale esterno, senza specifica autorizzazione del personale del servizio di supporto tecnico SIA. [Necessario seguire specifica procedura]

[5] Ad esempio, le 6 licenze di tipo Creative Commons, definite dalla combinazione di quattro attributi che permettono di stabilire esplicitamente quali siano i diritti riservati, modificando la regola di default in cui tutti i diritti sono riservati.

3) Non è consentito l'uso di software applicativi diversi da quelli distribuiti ufficialmente dal SIA (ai sensi del D.lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore), inclusi nel catalogo dei servizi e nella *white list.*
4) È vietato conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, e-mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo se di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.
5) Il trasporto al di fuori del perimetro aziendale di dispositivi di memorizzazione contenenti dati personali e sensibili è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
6) L'utilizzatore di sistemi e servizi IT è invitato alla immediata segnalazione al servizio di supporto tecnico di eventuali danni, perdita di funzionalità parziale o totale dei dispositivi o delle apparecchiature.
7) Eventuali specifiche indicazioni o istruzioni fornite dal personale di supporto tecnico devono essere rispettate al fine di garantire il miglior funzionamento possibile dei sistemi, dei dispositivi e delle risorse condivise.
8) Concluse le attività lavorative o nel caso di momentanea assenza o allontanamento dalla postazione di lavoro, l'utilizzatore di sistemi e servizi IT è tenuto alla disconnessione dei servizi e degli applicativi attivi o alla completa disconnessione/arresto del sistema (Windows-l (elle), blocco dell'utilizzatore connesso oppure Start – Arresta / Disconnetti).

Art. 20. - Utilizzo delle cartelle di rete, collegate e condivise

1) Le cartelle di rete, collegate e condivise, sono di 3 tipi:
    a. Cartella ad accesso personale (Disco X:) dove salvare i documenti ancora in lavorazione o non ancora da condividere;
    b. Cartella ad uso Unità Operativa (Disco Y:) per la condivisione tra gli utilizzatori appartenenti allo stesso gruppo/ufficio;
    c. Cartella progetto (Disco Z:) ad uso combinato tra più Unità Operative per la condivisione interdipartimentale;
    d. File hosting aziendale (es. NextCloud) per la condivisione via web.
2) L'utilizzatore dovrebbe utilizzare la Cartella ad accesso personale per la memorizzazione dei documenti; questo al fine di ridurre il rischio di perdita poiché i file salvati in locale sui personal computer non sono replicati (non è previsto un backup dei dati contenuti sui singoli PC) e in caso di problemi ai dispositivi di memorizzazione potrebbero andare irrimediabilmente persi.
3) Nelle cartelle condivise (es. ad uso UO) è possibile impostare stratificazioni dei permessi (es. un gruppo di utente legge e altri scrivono su una cartella, mentre il resto è ad accesso libero).
4) Le cartelle condivise sono replicate in sicurezza (backup) tutti i giorni; è garantita una *retention* (tempo di conservazione delle copie) generalmente di 4 settimane (verificare con i SIA di Area Vasta le singole garanzie di conservazione);
5) È vietato conservare file protetti dal diritto d'autore nelle cartelle condivise, come anche in tutti gli altri dispositivi di memorizzazione aziendale.
6) I marchi, i segreti commerciali o i diritti di brevetto devono essere conservati con particolari accortezze e ad accesso ristretto. Contattare il supporto tecnico per delucidazioni a riguardo.
7) Gli utilizzatori hanno invece il compito di:
    a. Contenere lo spazio disco occupato entro le quote assegnate;
    b. Eliminare i file non più utilizzati o duplicati (es. file1.vers1, file1.vers2);
    c. Evitare la duplicazione delle informazioni già contenute in applicativi specifici aziendali (export dei dati per successiva elaborazione su Excel, import dei dati in database Access).

Art. 21. - File hosting

1) Il file hosting di dati personali o riservati, riconducibili all'organizzazione su sistemi non aziendali come Google Drive, Dropbox, WeTrasfer è vietato.
2) È possibile utilizzare il sistema aziendale di condivisione disponibile all'indirizzo: https://filehosting.sanita.marche.it
3) Eventuali utilizzi di sistemi cloud o di altre piattaforme di condivisione deve essere specificatamente autorizzata dal dirigente di UOS/UOC e comunicata al SIA.

Art. 22. - *Cloud computing* e servizi IT esterni

1) L'acquisizione di servizi basati su tecnologia cloud come IaaS, PaaS e SaaS devono essere conformi alla normativa nazionale e alle Politiche di approvvigionamento che prevedono per servizi tecnologici l'autorizzazione da parte dei Sistemi Informativi dell'organizzazione. Considerati i possibili impatti sulla protezione dei dati è necessario informare preventivamente anche il DPO/RPD.
2) L'utilizzo di sistemi basati su tecnologia cloud o web non autorizzati e tracciati è considerato un data breach con tutti i risvolti sanzionatori ed eventualmente risarcitori a carico dell'utilizzatore.

Art. 23. - Utilizzo Reti Wi-Fi pubbliche

1) Per ragioni di sicurezza, non devono essere utilizzate reti Wi-Fi pubbliche con l'opzione di protezione WEP ma soltanto WPA o WPA2.
2) Utilizzare la connessione Wi-Fi pubblica solo per effettuare navigazione informativa; non accedere mai alle piattaforme aziendali. Sono inoltre sconsigliati l'effettuazione di transazioni di tipo sensibile (ad es. acquisti o transazioni bancarie).

Art. 24. - Utilizzo Reti Bluetooth

1) Il Bluetooth deve essere attivato soltanto quando necessario; alla fine della sessione di lavoro deve essere sempre disattivato.
2) Al fine di garantire un adeguato livello di sicurezza è necessario verificare l'ambiente circostante in modo che si possa considerare sicuro; devono quindi essere evitati i luoghi pubblici (con promiscuità inferiore ai 50 metri).
3) La visibilità del dispositivo via protocollo Bluetooth deve essere attivata solo se necessario alla prima fase di configurazione e registrazione; poi può essere disabilitato.
4) Attivare sempre le opzioni di sicurezza come l'autenticazione e la cifratura delle comunicazioni attraverso l'implementazione di protocolli sicuri.

Art. 25. - Sistemi di Sicurezza

1) L'organizzazione al fine di tutelare il patrimonio informativo e la continuità dei servizi, utilizza dei dispositivi di sicurezza con i quali controlla e monitora in modalità aggregata l'attività dei sistemi e indirettamente anche quella degli utilizzatori. Al fine di poter valutare i livelli di servizio erogati ed effettuare attività di ricerca forense a seguito di eventuali attacchi, tutte le attività dei sistemi e degli utilizzatori sono salvate in appositi registri o file di log, ai quali può accedere solamente il personale autorizzato e specificatamente nominato Amministratore di Sistema.
2) L'accesso ai file di log da parte del personale nominato Amministratore di Sistema può avvenire per attività di normale manutenzione, a seguito di malfunzionamenti o di degradamento dei livelli di servizio, in funzione di specifiche segnalazioni oppure nel caso di richiesta da parte dell'Autorità Giudiziaria.
3) La scelta dei criteri di protezione nei sistemi di sicurezza è teso al giusto equilibrio tra performance e livello di salvaguardia, proporzionale ai rischi connessi con la tipologia di informazioni trattate. In alcuni casi, i controlli possono interferire con l'esperienza dell'utilizzatore di sistemi e servizi IT, ad

esempio con blocchi nella navigazione, accessi non concessi, segnalazione di attività non permesse. L'utilizzatore di sistemi e servizi IT è invitato a segnalare gli elementi che ritiene possano essere migliorati (ad es. falsi positivi).

4) L'utilizzatore di sistemi e servizi IT non deve modificare, aggirare, disabilitare i controlli di sicurezza. Eventuali attività ritenute sospette comporteranno l'immediata disattivazione dell'account di accesso ai sistemi e servizi (questo poiché è impossibile per un sistema automatico stabilire con certezza se il problema è, o meno, riconducibile ad una compromissione, presentandosi come rischio inaccettabile e non risolvibile con altri mezzi).
5) L'accesso alle infrastrutture di rete, alle attrezzature e strumenti informatici è permesso al solo personale autorizzato; il personale privo di autorizzazione non può effettuare l'accesso, anche se accompagnato, senza preliminare autorizzazione e registrazione.
6) I sistemi o i dispositivi compromessi a seguito di attacco devono essere ripristinati dal personale dei Sistemi Informativi seguendo le procedure previste; la delega a terza parte necessita di specifica approvazione da parte di un soggetto Designato o dal Dirigente del SIA.
7) I sistemi e gli applicativi necessitano di continui aggiornamenti che permettono di mantenere l'intera infrastruttura ad un adeguato livello di protezione e sicurezza, eliminando i difetti o le vulnerabilità note. Nonostante tutte le accortezze, alcuni aggiornamenti richiedono molto tempo, rallentano il sistema o possono esigere un riavvio. L'utilizzatore di sistemi e servizi IT deve seguire quanto richiesto dal sistema o dall'applicazione nel più breve tempo possibile al fine di ridurre i rischi legati allo specifico aggiornamento.

Art. 26. - Sondaggi (telefonici e on-line)

1) Gli attacchi di tipo *Social Engineering* si basano sullo studio del comportamento individuale di una persona al fine di carpire informazioni utili e funzionali agli scopi malevoli; altra modalità più subdola è il tentativo di stabilire un certo livello di fiducia con la vittima in modo che riveli in autonomia le informazioni riservate necessarie agli scopi. Per questo motivo è vietato:
    a. Rispondere a e-mail, questionari on-line o ai sondaggi se non provenienti da fonti istituzionali verificate (es. connessione in https e certificato valido);
    b. Rispondere a interviste telefoniche anche se annunciate o provenienti dall'estero (eventualmente procedere con un call-back verificando sul web i chiamanti), specialmente nel caso di richieste di informazioni relative all'organizzazione, alle infrastrutture o ai prodotti tecnologici utilizzati.

Art. 27. - Accesso remoto (VPN)

1) L'acceso dall'esterno alla rete aziendale può avvenire soltanto in due modi:
    a. Utilizzando le piattaforme esposte sul web (es. Posta elettronica, Sito web, portale dipendenti ASUR, ecc.);
    b. Virtual Private Network (VPN).
2) La richiesta di attivazione di una VPN deve essere presentata dal diretto superiore dell'utilizzatore inviando lo specifico modulo al supporto tecnico del SIA. Devono inoltre essere specificate le macchine server o i dispositivi da raggiungere. A meno di particolarissime eccezioni autorizzate dal Dirigente del SIA, non sono fornite VPN ad accesso ampio o completo della rete dell'organizzazione.
3) L'autorizzazione deve essere rinnovata di anno in anno sempre attraverso la procedura di abilitazione. Gli account VPN non rinnovati sono automaticamente disabilitati alla fine del periodo.
4) La macchina su cui installare il client VPN deve essere:
    a. Protetta da password di una certa complessità;
    b. Esente da applicativi software non licenziati e da crack di sblocco delle applicazioni o dei componenti;

c. Aggiornata all'ultima versione disponibile di sistema operativo (i sistemi operativi in *out of support* devono essere dotati di sistema di *virtual patching* o comunque sostituiti/aggiornati il prima possibile);
d. Dotata di software antivirus, con basi di definizione aggiornate almeno giornalmente.

5) Il software VPN automaticamente disconnette l'utilizzatore dopo 30 minuti di inutilizzo della linea. È necessario effettuare di nuovo l'accesso per ristabilire la connessione. Non sono ammessi client di accesso se non quelli distribuiti con la fase di rilascio delle credenziali di accesso.
6) Gli utilizzatori delle connessioni VPN, dato che sono a tutti gli effetti estensioni della rete dell'organizzazione, devono sottostare in tutto e per tutto al presente regolamento.
7) Il team di sicurezza effettua periodici monitoraggi alle attività degli utilizzatori del servizio VPN attraverso *walk-thrus*, video monitoring, report, audit interni o esterni. Comportamenti non conformi o anche solamente sospetti negli accessi o durante le sessioni di lavoro, comporteranno la disabilitazione dell'account di connessione.
8) In caso di compromissione del sistema a causa di virus o *malware*, l'utilizzatore non deve collegarsi alla rete dell'organizzazione ma deve provvedere alla completa reinstallazione del sistema operativo e degli applicativi e componenti soltanto da fonti affidabili e perfettamente licenziati.
9) È permesso il salvataggio temporaneo dei file e documenti di lavoro nella postazione di proprietà personale a patto di provvedere quanto prima alla completa eliminazione.

Art. 28. - Controllo remoto

1) Parte dell'attività di supporto tecnico è effettuata attraverso sessioni di controllo remoto, sempre attivate/autorizzate dagli utilizzatori. Questa modalità permette un enorme risparmio di tempo, risposte molto brevi, facilità di comprensione e risoluzione dei problemi. Anche le sessioni di *learning by doing* sono effettuate in questa modalità, conformemente al detto confuciano "*Se ascolto dimentico, se vedo ricordo, se faccio capisco*". Gli strumenti di controllo remoto aprono delle porte verso l'esterno della rete aziendale che intrinsecamente sono un potenziale elemento di insicurezza, da regolamentare, controllare e governare.
2) Dato che gli strumenti di controllo remoto permettono di visualizzare a distanza delle attività che i lavoratori effettuano con i sistemi informatici, è fondamentale che:
   - Sia sempre l'utilizzatore a richiedere il supporto tecnico (interno o esterno) tramite controllo remoto, autorizzando specificatamente ogni sessione;
   - Al termine dell'attività di supporto o formazione tramite controllo remoto, lo stesso utilizzatore provveda alla disconnessione del sistema remoto, al fine di evitare inutili occupazioni di banda e peggio la trasmissione (remota) della propria successiva attività lavorativa.
3) I tecnici interni possono utilizzare esclusivamente gli strumenti omologati dal SIA aziendale e pubblicati nella specifica procedura di Controllo remoto; è sempre vietata l'impostazione di sessioni sempre attive di controllo remoto, l'utilizzo o l'installazione di strumenti alternativi a quelli previsti.
4) Eventuali eccezioni dovranno essere specificatamente autorizzate dal Dirigente SIA, poiché sono da considerarsi potenziali vulnerabilità nella rete aziendale.
5) Al fine di ridurre la superficie di esposizione e le vulnerabilità connesse con l'utilizzo di strumenti di controllo remoto saranno effettuati periodici scanning di rete in modo da verificare la presenza di applicazioni di controllo remoto non autorizzate o sempre attive. Le applicazioni di controllo remoto non conformi saranno rimosse.

Art. 29. - Pubblicazione di informazioni sui siti web istituzionali e Social media

1) ASUR utilizza i propri siti web e i social media con finalità istituzionali e di interesse generale per informare, comunicare, ascoltare e per consentire una relazione più diretta e una maggiore partecipazione dei cittadini alle attività svolte.

2) Attualmente la comunicazione ASUR avviene attraverso le pagine tematiche presenti su:
    a. www.asur.marche.it
    b. Facebook
    c. Twitter
    d. Instagram
    e. Telegram
    f. LinkedIn
    g. YouTube.

    In futuro non sono escluse ulteriori affiliazione ai social media (la lista sarà tenuta aggiornata rispetto alla gestione delle versioni del presente regolamento) o la registrazione di specifici domini web.
3) I contenuti che sono pubblicati sui siti web istituzionali e sui social possono comprendere comunicazioni sulle attività e i servizi erogati, comunicati stampa, pubblicazioni e documenti ufficiali, novità normative, informazioni su iniziative ed eventi di settore, immagini e video istituzionali e relativi a eventi a cui l'organizzazione partecipa.
4) I canali producono propri contenuti testuali, fotografie, informazioni grafiche, video e altri materiali multimediali che sono da considerarsi in licenza *Creative Commons* CC BY-ND 3.0 [Attribuzione – Non opere derivate http://creativecommons.org/licenses/by-nd/3.0/it/deed.it]: possono essere riprodotti liberamente, ma devono sempre essere accreditati al canale originale di riferimento.
5) I commenti e i post degli utenti, presentati preferibilmente con nome e cognome non fittizi, rappresentano l'opinione dei singoli e non quella dell'organizzazione, che non può essere ritenuta responsabile della veridicità o meno di ciò che viene postato sui canali da terzi, entità giuridiche o naturali.
6) I partecipanti alle discussioni sui social network sono responsabili dei contenuti pubblicati e delle opinioni espresse. Non sono comunque tollerati insulti, volgarità, offese, minacce. Devono essere evitati riferimenti a fatti o a dettagli privi di rilevanza pubblica, atteggiamenti violenti, offensivi o discriminatori rispetto al genere, orientamento sessuale, età, religione, convinzioni personali, origini etniche, disabilità. Messaggi contenenti dati personali (indirizzi e-mail, numeri di telefono, numeri di conto corrente, indirizzi, etc.) saranno rimossi a tutela delle persone interessate.
7) L'attività di moderazione da parte dell'amministratore del social può avvenire solo a posteriori in un momento successivo alla pubblicazione; l'attività è finalizzata, unicamente, al contenimento di eventuali comportamenti contrari alle norme d'uso, garantendo a tutti il diritto di intervenire ed esprimere la propria libera opinione.
8) Non sono tollerati comportamenti da cosiddetti *hater*, con insulti, turpiloquio, minacce o atteggiamenti che ledano la dignità personale, i diritti delle minoranze e dei minori, i principi di libertà e uguaglianza o altri principi costituzionalmente riconosciuti ed in particolare:
    a. Contenuti che promuovono, favoriscono, o perpetuano la discriminazione sulla base del sesso, della razza, della lingua, della religione, delle opinioni politiche, credo religioso, età, stato civile, nazionalità, disabilità fisica o mentale o orientamento sessuale;
    b. Contenuti sessuali o link (collegamenti) a contenuti sessuali;
    c. Pubblicità evidente o sollecitazioni commerciali;
    d. Incoraggiamento ad attività illecite;
    e. Informazioni che possono tendere a compromettere la sicurezza o la sicurezza dei sistemi pubblici;
    f. Contenuti che violino l'interesse di una proprietà legale o di terzi;
    g. Commenti o post che presentino dati sensibili in violazione della normativa sulla protezione dei dati personali;
    h. Sono inoltre scoraggiati e comunque soggetti a moderazione commenti e contenuti dei seguenti generi:

i. Spam, commenti non pertinenti agli argomenti trattati (*off topic*);
ii. Osservazioni pro o contro campagne politiche o indicazioni di voto;
iii. Linguaggio o contenuti offensivi;
iv. Commenti e i post scritti per disturbare la discussione, offendere chi gestisce e modera i canali social;
v. Interventi inutili o inseriti ripetutamente.

9) Gli utilizzatori che dovessero violare ripetutamente le condizioni sopra riportate o quelle contenute nelle specifiche policy degli strumenti adottati, potranno essere "bannati" o bloccati al fine di impedirne ulteriori interventi.
10) Le attività ritenute illegali saranno immediatamente comunicate alle autorità competenti.

Art. 30. - Formazione

1) L'utilizzatore di sistemi e servizi IT è tenuto a frequentare i corsi frontali, *blended* o in modalità e-learning considerati prerequisito di accesso ai servizi e agli applicativi, come anche di aggiornamento a seguito di introduzioni di novità rilevanti, siano essi organizzati dai Sistemi Informativi, tenuti dal personale interno o da esperti esterni.
2) L'utilizzatore di sistemi e servizi IT che compia azioni vietate dal presente regolamento, è obbligato a frequentare una specifica sessione di formazione dedicata ai temi connessi con la non conformità riscontrata. La sessione formativa è organizzata a cura dei Sistemi Informativi.
3) A conclusione di ogni intervento formativo (prerequisito, aggiornamento o *retraining*) è prevista la verifica delle competenze acquisite tramite test di valutazione. Nel caso in cui l'utilizzatore di sistemi e servizi IT non superi la prova con almeno l'80% delle risposte esatte, è obbligato a ripetere la formazione e il test, senza la possibilità temporanea di accesso all'ambiente di produzione del servizio o applicativo oggetto della formazione. Ove disponibile e se previsto, è possibile utilizzare specifici ambienti di simulazione per il miglioramento delle competenze.
4) Il Dirigente dei Sistemi Informativi, al fine di migliorare il livello di sicurezza, organizza con cadenza annuale delle sessioni di formazione ed aggiornamento dedicate al personale IT sui temi della sicurezza nel trattamento dei dati e su temi specifici connessi ai compiti di amministrazione di sistema.

CAPO III – Attori e ruoli

Art. 31. - Utilizzatore dei servizi e degli applicativi

1) L'Utilizzatore dei servizi e degli applicativi è un individuo espressamente autorizzato ad effettuare trattamenti di dati attraverso applicazioni software. Le autorizzazioni possono essere nominali o per funzione ovvero per appartenenza a uno specifico gruppo di lavoro.
2) Le autorizzazioni sono concesse dal Dirigente di Unità Operativa che individua ambito e profilo di autorizzazione con comunicazione al SIA, che provvede alle necessarie impostazioni a livello di sistema o di applicativo.
3) L'Utilizzatore dei servizi e degli applicativi deve attenersi scrupolosamente alle procedure operative indicate nei manuali d'uso, nelle note operative, negli aiuti in linea, illustrati durante le sessioni formative o comunicate durante il cosiddetto *learning by doing (imparare facendo).*
4) Gli utilizzatori dei servizi e degli applicativi hanno l'obbligo di segnalare immediatamente al proprio Dirigente qualsiasi evento o situazione di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo aziendale e garantire la necessaria continuità operativa.

Art. 32. - Dirigenti di UOS/UOC/Dipartimenti

1) Il Dirigente di Unità Operativa, in forza della nomina a soggetto Designato, provvede all'autorizzazione degli utilizzatori (incaricati del trattamento dei dati) individuando ambito e profilo di autorizzazione anche in funzione degli applicativi software in uso.
2) Con periodicità almeno annuale provvede alla verifica dell'ambito e del profilo di autorizzazione degli utilizzatori assegnati alla propria Unità Operativa, comunicando al SIA (Sistema Informativo Aziendale) le eventuali variazioni.
3) Il Dirigente di Unità Operativa ha l'obbligo di segnalare immediatamente al Dirigente del SIA eventuali anomalie o situazioni di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo aziendale e garantire la necessaria continuità operativa.

Art. 33. - Amministratori di Sistema

1) Il personale sistemistico e di networking, avendo facoltà di accesso alle informazioni anche senza i vincoli e le protezioni del livello applicativo, è nominato Amministratore di Sistema dal Dirigente del SIA o dal Dirigente Unità Operativa che provvede ad attribuire singolarmente l'ambito di autorizzazione. Sono considerati Amministratori di sistema i tecnici che lavorano a tutti i livelli della catena tecnologica al di sotto dello strato applicativo a meno che possano definire e rilasciare credenziali di autenticazione.
2) A partire dal livello "visibile", la catena tecnologica è composta da:
    a. Livello applicativo;
    b. Middleware (DBMS e web service);
    c. Sistemi operativi;
    d. Hypervisor;
    e. Server e sottosistemi SAN/NAS;
    f. Network.
3) I principali compiti di un Amministratore di Sistema sono i seguenti:
    a. Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
    b. Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
    c. Installare e configurare nuovo hardware/software sia lato client sia lato server;
    d. Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'organizzazione;
    e. Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
    f. Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di *troubleshooting*;
    g. Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
    h. Documentare le operazioni effettuate (*Logbook*), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
    i. Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
    j. Operare secondo le prescrizioni di sicurezza e le procedure interne previste.

Art. 34. - Chief Information Officer (CIO)

1) Il Dirigente del SIA o *Chief Information Officer* (*CIO*) è il manager responsabile delle tecnologie dell'Informazione e della Comunicazione. Il Dirigente del SIA verifica periodicamente e con cadenza annuale, l'attività degli Amministratori di Sistema attraverso audit interni, al fine di accertarne la conformità alle mansioni attribuite e la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti.
2) Il Dirigente del SIA redige annualmente la "Relazione sull'attività svolta dagli Amministratori di Sistema", i risultati degli audit interni, la conformità alle misure organizzative, tecniche e di

sicurezza previste dalle norme vigenti, riportando in evidenza tutti gli interventi volti a migliorare il livello complessivo di sicurezza.

3) Il Dirigente del SIA è direttamente coinvolto nella definizione delle strategie ICT e delle policy di gestione e innovazione dell'ICT aziendale, entrambi necessarie per la sicurezza del patrimonio informativo aziendale. È responsabile del governo del sistema informativo ovvero l'insieme delle attività promosse e gestite dal management e dai sistemi informativi, al fine di trovare la migliore integrazione possibile tra IT, *mission* e *vision* aziendali, in un'ottica di riduzione dei rischi:
   a) Raccogliere e razionalizzare le esigenze dei propri "Clienti Interni";
   b) Contribuire all'analisi e alla definizione dei processi aziendali;
   c) Contribuire alla definizione dei requisiti funzionali e architetturali degli strumenti informativi;
   d) Contribuire alla gestione del cambiamento dovuto all'introduzione di nuovi strumenti informativi;
   e) Definire e gestire il budget destinato ai Sistemi Informativi;
   f) Definire degli standard metodologici e tecnologici di riferimento;
   g) Definire metriche (KPI, SLA) per la valutazione dell'efficienza interna e dei fornitori di software e servizi;
   h) Organizzare e gestire il funzionamento quotidiano dei sistemi informativi, ottimizzando le risorse interne e gli appalti verso fornitori esterni;
   i) Organizzare e gestire il flusso delle informazioni sulla base dell'esperienza agevolando l'uso della tecnologia nel complesso informativo;
   j) Sviluppare e implementare nuove policy e procedure specifiche per Unità Operative e promuovere la conformità;
   k) Gestire la conformità ai requisiti del modello di *governance* adottate dall'organizzazione;
   l) Garantire la sicurezza dei sistemi informatici e la rete a cui sono collegati;
   m) Fornire i nuovi dipendenti delle necessarie istruzioni/procedure rispetto alle mansioni svolte e agli strumenti utilizzati;
   n) Mantenere la funzionalità dei sistemi informatici nelle varie aree;
   o) Impedire l'accesso non autorizzato alle informazioni aziendali, file personali ed e-mail;
   p) Provvede allo sviluppo e il mantenimento di un piano per il recupero dei sistemi e dei dati critici.

Art. 35. - Fornitori di prodotti e servizi

1) I fornitori di prodotti e servizi del SIA sono coloro che provvedono all'approvvigionamento di beni o alla prestazione di servizi all'organizzazione. In fase di appalto, dichiarano di accettare le regole e le procedure del presente regolamento.
2) In caso di *outsourcing* di un servizio relativo a un sistema oppure ad un applicativo, il personale tecnico è nominato Amministratore di Sistema dal titolare dell'azienda appaltatrice, che nello specifico svolge il ruolo di Responsabile (esterno) del trattamento ai sensi dell'art. 28 del GDPR. Almeno una volta l'anno, il titolare dell'azienda appaltatrice comunica al Direttore del SIA l'elenco degli Amministratori di Sistema nominati e autorizzati a effettuare il servizio relativo all'appalto.

Art. 36. - Data Protection Officer (DPO)

1) Il DPO ha le seguenti responsabilità (oltre a quanto già previsto dall'art 39 del GDPR):
   a. Sensibilizzare e formare il personale in modo da garantire un adeguato livello di consapevolezza sulle minacce alla sicurezza informatica;
   b. Gestire le procedure di data breach;
   c. Fungere da punto di contatto con l'Autorità Garante della protezione dei dati personali.

Art. 37. - Cyber Security Team

1) Il team Cyber Security è composto da personale tecnico dei Sistemi Informativi Aziendali specificatamente formato sulle tematiche della sicurezza informatica.
2) Il team Cyber Security ha le seguenti responsabilità:
    a. Attivare le procedure di emergenza nei casi previsti;
    b. Gestire il ritorno alla normalità dopo un evento di sicurezza;
    c. Implementare le logiche di sviluppo continuo e miglioramento delle difese informatiche;
    d. Intraprendere un monitoraggio e una revisione continui delle pratiche e delle difese.

Art. 38. - Comitato rischi, audit e conformità

1) Il Comitato per il rischio, l'audit e la conformità è composto da:
    a. Chief Information Officer (CIO)
    b. Data Protection Officer (DPO)
    c. Cyber Security Team
2) Il comitato per il rischio, l'audit e la conformità ha le seguenti responsabilità:
    a. Monitorare i rischi e i controlli di sicurezza informatica esaminando i risultati dei processi di gestione dei rischi informatici e monitorando i rischi emergenti;
    b. Supervisionare l'adeguatezza delle capacità e dei controlli di sicurezza informatica.

Art. 39. - Responsabile per la transizione digitale

1) Il Responsabile della Transizione al Digitale (RTD) è la figura dirigenziale all'interno della PA che ha tra le sue principali funzioni quella di garantire operativamente la trasformazione digitale dell'amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di nuovi modelli di relazione trasparenti e aperti con i cittadini.
2) All'ufficio del RTD sono attribuiti i compiti di:

    a) Coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia;
    b) Indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
    c) Indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;
    d) Accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità;
    e) Analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
    f) Cooperazione alla revisione della riorganizzazione dell'amministrazione;
    g) Indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
    h) Progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
    i) Promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) Pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione;

k) Pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione, al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale ed in particolare, con quelli stabiliti nel piano triennale.

CAPO IV – Gestione delle emergenze

Art. 40. - Evento di sicurezza e Risposta

1) Un Evento di sicurezza è definito come un cambio di stato avente rilevanza ai fini della gestione di un asset o di un servizio IT. Il cambio di stato potrebbe configurare l'insorgere di un malfunzionamento, di un incidente da gestire ai sensi del successivo articolo oppure risultare come normale attività da gestire (es. completamento di un backup).
2) L'Evento di sicurezza deve essere analizzato dal personale di supporto di primo livello e, nel caso si tratti di una eccezione, deve essere assegnato al supporto di secondo livello per la prevenzione/gestione del problema o dell'incidente.
3) Il personale di supporto di primo livello gestisce gli eventi di sicurezza senza registrare ticket a meno che vi sia una gestione automatica delle registrazioni, nel caso si tratti di evento potenzialmente rilevante per la continuità operativa o impattante sui livelli di servizio previsti.

Art. 41. - Incidente di sicurezza e Risposta

1) Un incidente è definito come un qualsiasi evento eccezionale non facente parte delle operatività standard di un servizio; può causare una riduzione della qualità del servizio o provocarne l'interruzione.
2) In tutti i casi di incidente di sicurezza deve essere informato il Direttore del SIA che, nei casi più gravi, procederà ad informare la Direzione Generale.
3) Il personale di supporto di primo livello, una volta identificato l'incidente, lo registra nel sistema di ticketing e allerta immediatamente il personale di supporto di secondo livello; nei casi più gravi avverte la squadra di salvataggio (*rescue team*) composta anche da personale esterno specializzato nelle tecnologie coinvolte dal problema, al fine di risolvere il più velocemente possibile la situazione riportando i livelli di servizio alla condizione precedente.
4) Il *rescue team* procede alla classificazione dell'incidente effettuando una approfondita analisi e diagnosi dell'incidente, procedendo secondo delle soluzioni documentate e preimpostate o tramite attività di *workaround* (soluzione momentanea).
5) Una volta risolte le cause dell'incidente e riportato alla normalità il livello di servizio erogato, il rescue team procede con la chiusura dell'incidente e con la documentazione delle modalità di risoluzione. È avvertito anche il Direttore del SIA che procede con le comunicazioni ai soggetti coinvolti, inclusa la Direzione Generale e il DPO/RPD per i casi più gravi o impattanti dal punto di vista dei diritti degli interessati.

Art. 42. - Data breach e Risposta

1) Una violazione di sicurezza sui dati personali o data breach è un evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati avvenuto in modo accidentale oppure in modo illecito.

2) Ai sensi di quanto stabilito dall'art. 33 del GDPR, in caso di Data Breach è necessario seguire la prevista procedura che prevede tra l'altro, nei casi più gravi, la comunicazione all'Autorità Garante entro 72 ore dal momento in cui se ne è avuta conoscenza.
3) In tutti i casi è necessario avvertire il DPO/RPD che provvederà a documentare l'avvenuta violazione nel registro dei Data Breach.

Art. 43. - Sanzioni

4) Le operazioni effettuate in palese non conformità al presente Regolamento, esporranno alle sanzioni amministrative, civili e penali previste dalla normativa vigente.
5) Il mancato rispetto o la violazione di quanto previsto dal presente Regolamento, tenuto conto del principio di proporzionalità, è perseguibile con i seguenti provvedimenti disciplinari:
    a. Comunicazione dell'illecito alla Direzione che provvederà all'applicazione di quanto previsto alla determina 21/DG 2015 (Regolamento Disciplinare – personale comparto e Dirigenza).

Art. 44. - Prescrizioni

1) L'attività di gestione e utilizzo degli strumenti informatici e dell'infrastruttura di rete segue le norme del presente Regolamento.
2) Il presente Regolamento è distribuito a tutto il personale e a tutti gli esterni coinvolti nelle attività di utilizzo, gestione e manutenzione dei sistemi e dei dispositivi.
3) Gli utilizzatori sono informati sul presente Regolamento, pubblicato in Intranet; saranno inoltre fissate annualmente delle sessioni formative e di aggiornamento per i nuovi assunti in modalità frontale o e-learning.
4) Gli utilizzatori esterni devono essere debitamente informati sul presente Regolamento prima di poter accedere ai sistemi o alla rete di comunicazione, secondo le procedure previste.
5) Annualmente ed in base all'innovazione tecnologica o a sopravvenute esigenze sia organizzative che di sicurezza, si provvederà alla revisione del presente Regolamento e alle procedure allegate.

Art. 45. - Allegati

1) Le Procedure SIA fanno parte integrante del presente Regolamento.

2) Le procedure sono sviluppate, raccolte e diffuse a cura del SIA. Nella specifica sezione Procedure SIA presente nella piattaforma Intranet aziendale sono contenute solo le ultime versioni e revisioni aggiornate.

3) Al fine di evitare disallineamenti nella distribuzione delle procedure è sconsigliata la stampa: è necessario fare riferimento sempre all'ultima versione digitale pubblicata nella piattaforma Intranet.

4) Ogni procedura è composta dalle seguenti sezioni (le obbligatorie sono riportate in grassetto):

    1. **Scopo** (obiettivi generali della policy)
    2. **Campo di applicazione** (dove la policy è applicabile)
    3. Responsabilità (chi fa cosa)
    4. Riferimenti normativi e legislativi
    5. Background (motivazione che hanno portato alla redazione della policy)
    6. **Modalità operative** (descrizione delle attività)
    7. Controlli e verifiche (Indicatori di efficienza ed efficacia)
    8. **Gestione delle Revisioni**
    9. **Richieste** (a chi inviare eventuali richieste o integrazioni)
    10. Termini e definizioni (glossario dei termini e degli acronimi)
    11. Allegati (modulistica)

Art. 46. - Modulistica

1) La modulistica di riferimento aggiornata all'ultima versione e revisione è reperibile nella Intranet aziendale.

Glossario

VPN	Rete privata virtuale; modalità di collegamento sicuro alla rete aziendale
DMZ (zone demilitarizzate)	Sottorete isolata a livello fisico o logico nella quale sono pubblicati dei servizi informatici accessibili da LAN che da WAN
Hosting	Allocazione di un servizio o applicativo su un server pubblicato in Internet
Housing	Locazione di uno spazio fisico, generalmente all'interno di appositi armadi detti rack
Facility	Infrastrutture necessarie al funzionamento di un datacenter
Middleware	Software intermediari che permettono la comunicazione tra protocolli e sistemi operativi differenti
Wi-Fi	Rete wireless
BYOD	Bring your own device – dispositive personali utilizzati dai dipendenti per fruire di informazioni e applicazioni
instant messaging	Sistemi di comunicazione in tempo reale in rete
log	Sistema o modalità di registrazione degli eventi
Logbook	Contenitore dei log
keylogger	Malware in grado di registrare tutti i caratteri registrati da tastiera
firewall	Sistema di protezione dai pericoli della rete Internet
antispam	Sistema di filtraggio della posta indesiderata
phishing	Tipologia di attacco in cui si induce la vittima a fornire informazioni
forward	Re-invio automatico o manuale di un messaggio
CAD	Codice dell'Amministrazione Digitale
Smart card	Dispositivo hardware con potenzialità di elaborazione e memorizzazione dati in grado di garantire elevati standard di sicurezza.
SDI	Sistema di Interscambio per la Fatturazione elettronica PA
device wipe-out	Modalità di cancellazione totale o parziale dei contenuti per motivi di sicurezza di un dispositivo in caso di perdita dello stesso
Content Filtering	Filtraggio della navigazione Internet in modo da evitare siti web non allineati con gli obiettivi aziendali
Hacking	Metodi, tecniche e operazioni volte a conoscere, accedere e modificare un sistema informatico
plug-in	Programma non autonomo che interagisce con un altro programma per ampliarne o estenderne le funzionalità originarie
packet shaping	Modalità di adattamento della comunicazione in base a politiche di miglioramento del servizio
criptazione	"offuscare" un messaggio o un documento in modo da non essere comprensibile/intelligibile alle persone non autorizzate
retention	Tempistiche di conservazione dei backup
IaaS, PaaS e SaaS	Rispettivamente infrastrutture, piattaforme e software erogabili *on demand* sul cloud
Social Engineering	Studio del comportamento individuale di una persona al fine di carpire informazioni utili.
Retraining	Ripetizione della formazione prevista per uno specifico argomento
troubleshooting	Processo di ricerca logica e sistematica delle cause di un problema su un prodotto o processo affinché possa essere risolto

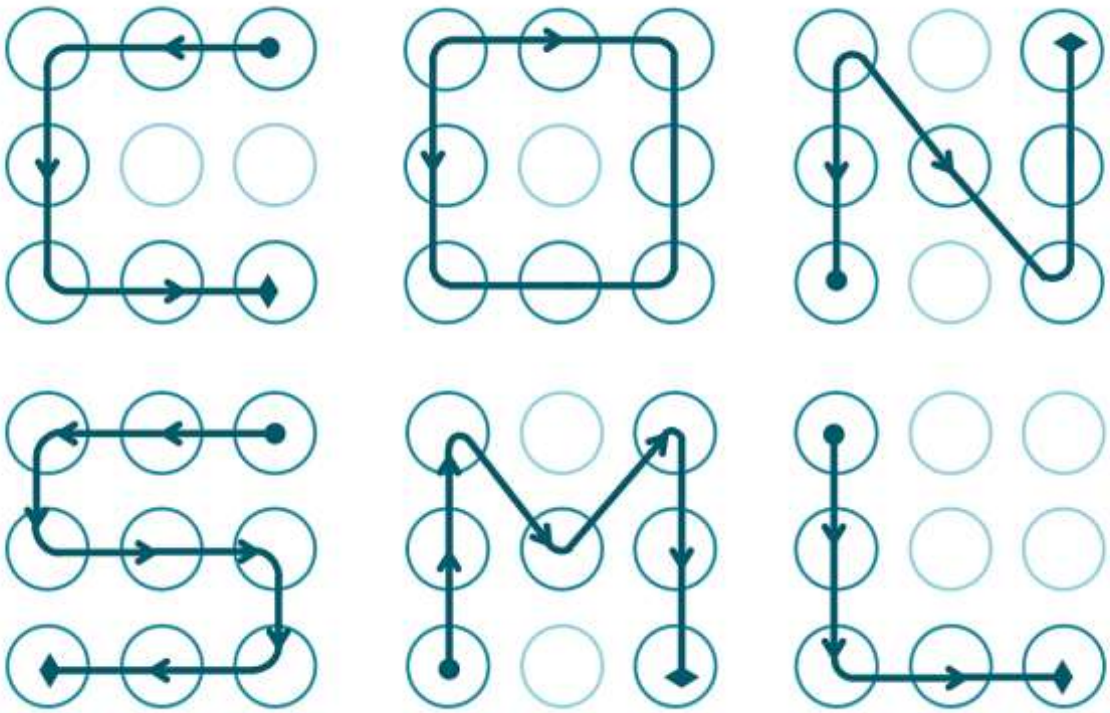
Appendice 1 - Password presenti nei dizionari pubblici

In ordine di frequenza rilevata:

1) Password
2) 123456
3) 123456789
4) Qwerty
5) password
6) 1111111
7) 12345678
8) abc123
9) 1234567
10) 1234567890
11) 9876543210
12) password1
13) 12345
14) letmein
15) football
16) iloveyou
17) admin
18) welcome
19) monkey
20) login
21) starwars
22) 123123
23) dragon
24) passw0rd
25) master
26) hello
27) freedom
28) whatever
29) qazwsx
30) trustno1

Le password riportate in questo elenco NON DEVONO essere utilizzate.

Appendice 2 – Combinazioni “FACILI” di sblocco smartphone e tablet



Le combinazioni di sblocco riportate in questo elenco NON DEVONO essere utilizzate.

PIN più utilizzati (4 cifre)

1234	1111	0000	1212
7777	1004	2000	4444
2222	6969	9999	3333
5555	6666	1122	1313
8888	4321	2001	1010

I PIN riportati in questo elenco NON DEVONO essere utilizzati.

Appendice 3 – Categorie di *Content Filtering*

Le seguenti tipologie di siti web non sono navigabili con gli strumenti messi a disposizione dell'organizzazione:

- Adult / Mature Content
- Bandwidth Consuming
- General Interest – Business
- Potentially Liable
- Security Risk