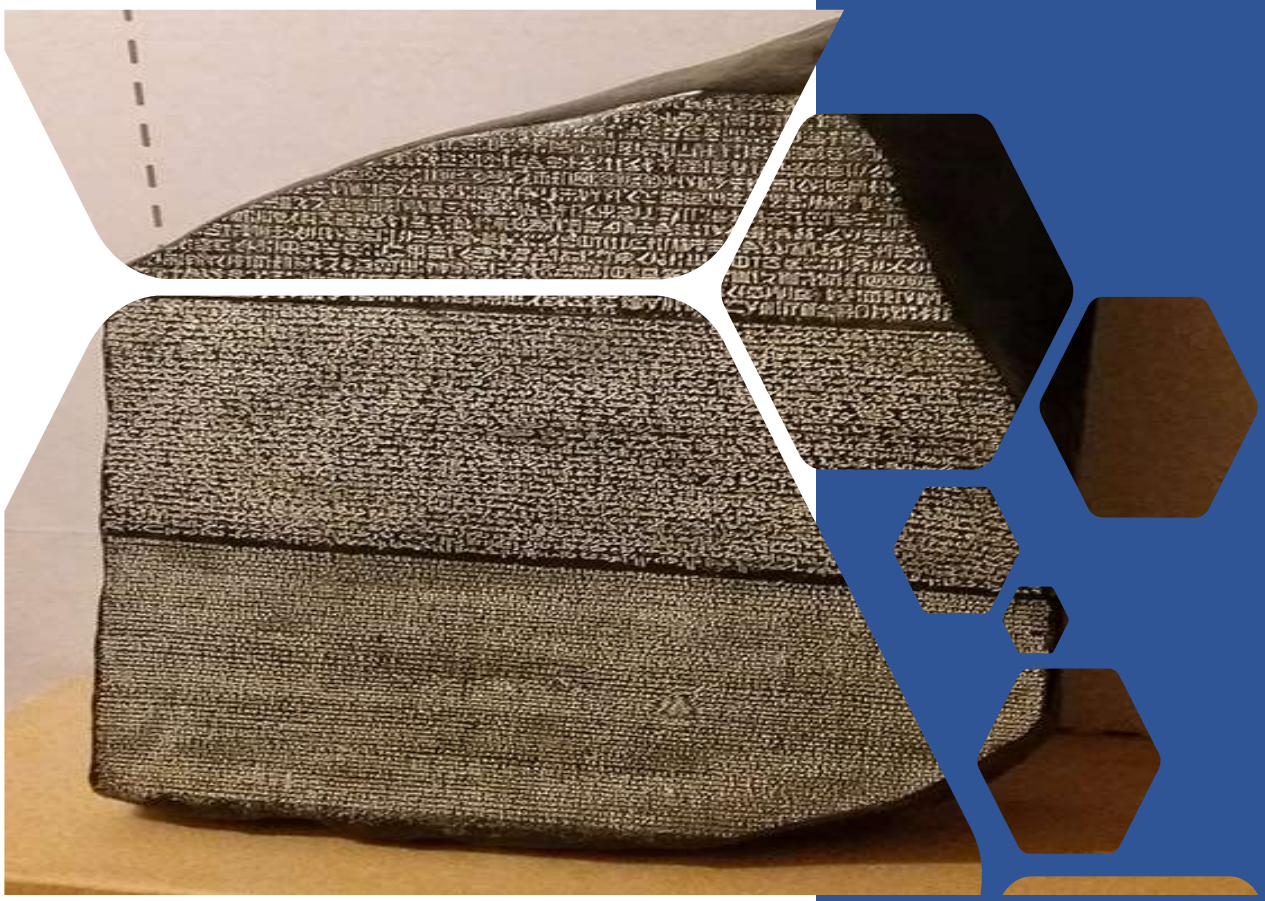
REGOLAMENTO UTILIZZO SISTEMI E SERVIZI IT



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

Chiave decisiva per la comprensione dei geroglifici

Sommario

Premessa

Quando il dipendente si imbatte suo malgrado con un qualsiasi tipo di regolamentazione (ancor peggio se si tratta di procedure in ambito *Information Technology*) è subito attraversato da un fremito anti-organizzazione, antiburocrazia, antisistema. I peggiori sono sempre gli informatici che, abituati alla massima libertà nella gestione tanto dei sistemi che degli applicativi, mal digeriscono limiti, imposizioni e ancor meno la necessità di documentare tutto quanto fatto.

In ambiti organizzativi molto evoluti che hanno sposato *best practice* internazionali, vale piuttosto il principio inverso e cioè "*If it wasn't documented, it wasn't done*" (letteralmente *non documentato = non fatto*); e questo al di là delle modalità, del peso, degli effetti e del livello di invasività potenziale o effettiva dei controlli.

La normativa vigente, europea e italiana, individua i 4 fattori determinanti per una qualsiasi soluzione applicativa o infrastruttura informatica ovvero Riservatezza, Integrità, Disponibilità e con gli ultimi aggiornamenti anche Resilienza. I primi 3 sono gli elementi della sicurezza dell'informazione definiti in letteratura mentre il quarto riguarda meccanismi di continuità operativa.

Tutti i procedimenti amministrativi sono oramai svolti con i sistemi informatici: l'inutilizzabilità di una soluzione applicativa blocca l'attività del personale, dato che nella maggior parte delle organizzazioni non sono mai state definite delle procedure alternative, talvolta non lo sono neanche quelle di emergenza per il recupero dai disastri e il ritorno alla normalità.

Se si considera che la maggior 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. L'obiettivo è prevenire lavorando sui singoli, sulle competenze e sui comportamenti non conformi che espongono tutta l'organizzazione a sanzioni, risarcimenti, peggio a danni reputazionali e di immagine.

In un ipotetico mondo dall'organizzazione perfetta gli strumenti di protezione risulterebbero totalmente inutili poiché le minacce non arriverebbero mai a sfruttare le vulnerabilità. Al contrario, risultano obbligatori (e spesso neanche sono sufficienti) per raggiungere un livello di sicurezza adeguato, peraltro previsto dalla normativa vigente sulla protezione dei dati personali.

Il tentativo del presente regolamento è di rendere facile, semplice, agile, snella qualsiasi attività legata alla gestione dei sistemi informatici da un lato, irrobustire il sistema di sicurezza, ridurre la superficie di esposizione ma prima di tutto rendere consapevoli gli operatori tanto dei rischi quanto della necessità delle contromisure, che troppo spesso appaiono invadenti, interferendo con l'attività degli utenti.

Buona sicurezza (*regolamentata*) a tutti.

Approccio metodologico

L'obiettivo di un regolamento è la definizione della disciplina relativa a un argomento come anche la specifica delle modalità di funzionamento di un sistema tecnologico o organizzativo.

Una modalità abbastanza standard di redazione prevede la declinazione dei principi generali che hanno richiesto o suggerito la regolamentazione, una successiva parte attuativa, e gli allegati, utili nella comprensione della relativa applicazione pratica.

Di solito tra i principi e la parte attuativa vi sono sempre delle aree grigie, vuote o non incluse, poiché la tendenza di chi redige il documento è la copertura delle problematiche contingenti e non una più generale strategia di governo. La bontà dei risultati di questo tipo di approccio dipende fortemente dalle esperienze, in grado di garantire quel livello di esperienza necessaria a concretizzare nel dispositivo normativo i passaggi utili ad evitare, per quanto possibile, il ripresentarsi di quanto già capitato in passato.

La redazione di un Regolamento per l'utilizzo dei sistemi e dei 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 al fine di tutelare il patrimonio informativo, prevenire problemi reputazionali o danni di immagine collegati ad usi impropri degli strumenti. Il proposito riguarda anche la sensibilizzazione, formazione e informazione al personale riguardo a tematiche sempre nuove legate all'innovazione che, visti i ritmi evolutivi, creano dei veri e propri dislivelli culturali difficilmente colmabili, tra quanto necessario ed effettivamente disponibile.

La regolamentazione che segue modifica radicalmente l'approccio tradizionale, introducendo una metodologia più rigorosa e basata, come tante norme di settore, sull'analisi dei rischi che incombono tanto sull'organizzazione quanto sui sistemi.

In modo forse non canonico ma funzionale, si è partiti dalle sorgenti, dalle potenziali minacce e vulnerabilità integrando progressivamente con casistiche effettivamente avvenute.

In altre parole, pur mantenendo l'asse sui principi generali, il focus è rivolto alla costruzione di uno strumento che possa fungere più da vademecum volto all'educazione degli utilizzatori piuttosto che ad uno strumento normativo di repressione delle cattive pratiche. Un'azione di sensibilizzazione e prevenzione piuttosto che di cura a posteriori.

Le sorgenti di rischio utilizzate sono ufficiali poiché provengono da:

- ENISA (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport)
- NIST Risk Management Framework (https://csrc.nist.gov/Projects/risk-management)

Gli articoli seguenti hanno l'obiettivo di attivare una nuova consapevolezza rispetto alla superficiale conoscenza degli strumenti tecnologici e dei rischi connessi; questo funzionalmente agli obiettivi tanto dell'organizzazione che dei singoli utilizzatori.

I pericoli sottesi agli articoli del presente regolamento sono seri e in grado di produrre danno enormi in termini funzionalità dei sistemi e riservatezza delle informazioni. I divieti non dovrebbero essere percepiti dal lettore in termini di costrizione ma soltanto di prevenzione, vere e proprie contromisure rispetto ai rischi legati al mondo dell'Information Technology.

Articolazione del Regolamento

Il Regolamento è organizzato con una prima parte introduttiva dove sono identificate e definite le componenti del sistema di gestione nel suo complesso. A seguire sono riportate per ogni tipologia di servizio o sistema le corrette modalità di utilizzo.

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

CAPO I - Disposizioni generali

Art. 1. - Oggetto e finalità

1) INRCA da anni è fortemente impegnata in importanti investimenti nell'ambito dell'innovazione, e nello specifico, nelle tecnologie e servizi dell'informazione per supportare le funzioni di prevenzione, diagnosi, cura, riabilitazione e ricerca, unite alle attività amministrative e di gestione dei servizi.
   Il presente Regolamento definisce il modello comportamentale considerato accettabile previsto per gli utilizzatori dei servizi e dei sistemi informatici dell'organizzazione e, inoltre, rappresenta idonea informativa ai sensi della vigente disciplina sulla protezione dei dati personali per quei trattamenti connessi con le attività di monitoraggio e controllo.
2) Al fine di preservare la continuità operativa dei servizi e il patrimonio informativo dell'organizzazione, ridurre i rischi di esposizione dal punto di vista sanzionatorio e risarcitorio rispetto alle normative nazionali ed europee vigenti come il GDPR, INRCA richiede agli utilizzatori dei servizi e sistemi informatici di conformarsi ai dettami del presente Regolamento come requisito obbligatorio di utilizzo.

Art. 2. - Ambito di applicazione - Perimetro

1) Il presente Regolamento si applica a tutti gli usi 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) diretta, i tunnel IPSec e i sistemi posizionati in zone demilitarizzate (DMZ), in *hosting*, in *housing* o in cloud (IaaS/PaaS/SaaS, privato/pubblico/di comunità/ibrido).
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, sistemi di monitoraggio e di controllo, i dispositivi client come i personal computer, i *thin client*, le stampanti multifunzione, i sistemi medicali, gli smartphone e i tablet, nonché apparati di telecontrollo e IoT (*Internet of Things*).
3) Sono escluse dal perimetro tutte le reti Wi-Fi di tipo *guest* a disposizione del pubblico nelle aree di Front Office e gli eventuali dispositivi collegati.
4) I sistemi e i dispositivi utilizzati dagli utenti al di fuori della rete INRCA per l'accesso ai servizi esposti in Internet sono esclusi dal perimetro (ad esempio, sono esclusi coloro che al di fuori della rete INRCA visitano i siti web istituzionali).

Art. 3. - Applicazione del Regolamento IT

1) Gli utenti sono obbligati a conformarsi al presente Regolamento come condizione di accesso e di utilizzo dei servizi e dei sistemi IT.
2) L'obiettivo del presente Regolamento è consentire un utilizzo legittimo e ottimale dei servizi e dei sistemi IT, sia al personale deputato alla gestione che a tutti gli utilizzatori.

Art. 4. - Definizioni

Ai fini del presente regolamento s'intende per:

1) **Minaccia**: qualcosa di potenzialmente pericoloso; possibili eventi non desiderati che portano alla perdita di riservatezza, integrità o disponibilità delle informazioni;
2) **Vulnerabilità**: caratteristiche dei sistemi e dei processi che, in particolari condizioni, possono comportare la perdita di riservatezza, integrità o disponibilità delle informazioni;
3) **Contromisure:** azioni di prevenzione e mitigazione individuate al fine di limitare probabilità ed impatto del rischio;

4) **Rischio:** probabilità che una minaccia si attui su un bene sfruttando una vulnerabilità; funzione rispetto a probabilità, impatto;
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 osservabile il normale comportamento di un sistema, ambiente, processo, flusso di lavoro o di una persona;
7) **Conseguenza:** Esito di un evento in grado di influenzare gli obiettivi;
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);
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 medesimo (coppia account utente e password);
11) **Spam**, posta spazzatura (in inglese *junk mail*)*:* invio di messaggi indesiderati ripetuti e frequenti, oppure monotematici (es. pubblicità);

Art. 5. - Principi

1) I principi ispiratori del presente regolamento sono i seguenti:
   a) Tutela dei diritti, delle libertà e della dignità delle persone;
   b) Garanzia della necessaria *continuità operativa* per l'erogazione del miglior servizio possibile unito al minor dispendio di energie (umane, tecnologiche, temporali ed economiche);
   c) Tutela del patrimonio informativo dell'organizzazione 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, allineamento agli standard di mercato e alle migliori pratiche;
   e) Security e privacy by design ovvero considerare la sicurezza e la conformità alla protezione dati personali come parte integrante della progettazione complessiva del sistema;
   f) Approccio alla sicurezza di tipo multilivello (*Layered security*), adottando tecniche di segmentazione e segregazione quanto maggiormente possibile;
   g) Protezione del patrimonio informativo in ogni fase del trattamento e per tutto il ciclo di vita, ovvero quando i dati sono elaborati e comunicati ("*data in transit*") o quando sono conservati ("*data at rest*" o "*in storage*");
   h) Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia, partendo dal modello "tutto chiuso":
   i) Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
   j) Adozione della Regola del minimo previlegio rispetto alla finalità (*Separation of duties policy*), in ottica di stratificazione dei profili e degli accessi;
   k) Consapevolezza di tutti gli utilizzatori rispetto ai rischi e alle corrette modalità di utilizzo dei sistemi e dei servizi IT.

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

1) I sistemi e i servizi IT sono forniti agli utenti per condurre e supportare la missione dell'organizzazione, ovvero le attività legate agli ambiti di ricerca, sanitari e/o amministrativi.

2) 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.
3) L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli account concessi, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio personal computer, applicativo software o piattaforma web.
4) All'utilizzatore di sistemi e servizi IT non sono consentite 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;
    c. la trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri;
    d. L'invio di dati di tipo sensibile su canali non sicuri (ad esempio la posta elettronica aziendale, che potrebbe viaggiare in chiaro quando inviata ad altro dominio di posta);
    e. La creazione, la memorizzazione e 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;
    g. L'utilizzo a fini personali dei sistemi, dispositivi o servizi forniti dall'organizzazione.
5) 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*), a meno di specifica autorizzazione di soggetti apicali.

Art. 7. - Tipologie di minacce

1) Una prima suddivisione delle minacce è riferibile alla sorgente:
    - Accidentale
    - Deliberata
    - Naturale

    Al di là delle motivazioni di chi intenzionalmente tenta di accedere abusivamente alle informazioni, esiste un problema di prevenzione rispetto a comportamenti ritenuti "normali" ma che nell'ambito dell'organizzazioni aumentano il livello di esposizione ai rischi connessi con i trattamenti di dati, specialmente quando si parla di dati personali o sensibili.
    Altra importante valutazione da fare, connessa con la continuità operativa, riguarda la riduzione dei rischi legati alle minacce di tipo naturale, tanto imprevedibili quanto devastanti.
2) Un secondo livello di suddivisione secondo l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) è la seguente:
    - Attacco fisico (deliberato / intenzionale)
    - Danni / perdite involontari di informazioni o risorse IT
    - Disastri (naturali, ambientali)
    - Interruzioni
    - Intercettazione / dirottamento
    - Attività / abusi con effetti nefasti
    - Conformità Legale

Art. 8. - Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

1) Un SGSI, secondo le norme ISO e in particolare rispetto alla famiglia ISO 2700x, è un insieme di politiche e procedure per la gestione sistematica dei dati rilevanti di un'organizzazione. L'obiettivo

di un SGSI è ridurre al minimo i rischi e garantire la continuità aziendale limitando proattivamente l'impatto di una violazione della sicurezza. Il presente regolamento come anche la modulistica IT sono parte integrante del SGSI.

CAPO II - Strumenti

Art. 9. - Identificazione, autenticazione e autorizzazione

1) L'organizzazione implementa nella gestione dei sistemi e i 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, o ai sistemi ad alta rotazione e intensità dove sono previsti account di accesso multiutente (cosiddetti account generici) e successivamente sono tracciate le singole registrazioni 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) ha effettuato 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 e alle specifiche mansioni assegnate.
4) La responsabilità delle azioni effettuate utilizzando la coppia "nome utente e password" sarà attribuita all'utilizzatore titolare registrato, a meno di comprovato illecito da parte di terzi. Sono escluse le attività di supporto in controllo remoto 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 fine del rapporto di lavoro.
6) A carico del soggetto designato permane l'obbligo di attivazione iniziale dell'account dell'utilizzatore dei sistemi e servizi informatici nonché di comunicazione di qualsiasi variazione del profilo autorizzativo, inclusa la disabilitazione.
7) Gli account di accesso hanno comunque una scadenza corrispondente a 10 giorni successivi alla data di fine del contratto, convenzione, accordo, autorizzazione. È a carico del Soggetto designato comunicare al personale dei Sistemi Informativi l'eventuale prolungamento del contratto e la necessità di estensione temporale delle autorizzazioni.
8) Gli Amministratori di Sistema gestiscono gli account utente per tutto il ciclo di vita (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, disabilitazione alla fine del rapporto di lavoro).
9) 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.).
10) 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 nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni.

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, 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, a meno della cosiddetta prevista *retention* dei sistemi di backup; in ogni caso la conservazione è strettamente limitata al perseguimento delle finalità organizzative, produttive e di sicurezza.
3) Alcuni file di log (es. accesso alla rete) sono conservati per almeno 2 anni dall'evento.
4) L'eventuale prolungamento dei tempi di conservazione è valutato sempre come eccezione, attuabile soltanto in relazione:
    a. ad esigenze tecniche o di sicurezza del tutto particolari;
    b. all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
    c. all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.
5) Il connesso trattamento di dati personali è comunque limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed è effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità.

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. Non è consentito 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" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.
2) La lunghezza minima di una 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 12 caratteri per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e 14 caratteri per le attività di amministrazione di sistema.
3) 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@).
4) 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, dell'organizzazione e personali riconducibili allo stesso soggetto.
5) 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*).
6) Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, essere troppo ovvie (es. 'P@ssword').
7) 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. (l'elenco non è esaustivo).
8) Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (criteri di complessità).

9) 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 di seguito riportate:
    a. Lunghezza minima 12 caratteri (14 caratteri per attività di amministrazione dei sistemi);
    b. Composizione articolata (complessità) con almeno una lettera maiuscola e una lettera minuscola, un numero e un carattere speciale;
    c. Modificate ogni 3 mesi (cd. *password aging*);
    d. Non riutilizzate a breve distanza di tempo con rotazione almeno pari a 5 e per almeno 12 mesi (cd. *password history*);
10) Le password non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.
11) La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti.
12) 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.
13) Non è consentita la memorizzazione delle password nei browser o tramite applicativi di gestione password (es. Pocket Password) 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.
14) Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile a quella utilizzata che si vorrebbe utilizzare per verificarne la robustezza; es. https://password.kaspersky.com/it/).
15) Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso media (es. la password può essere comunicata a voce, via telefono).
16) 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 - Appendice 3 - Password presenti nei dizionari pubblici).
17) 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, su ambiente Citrix il cambio password va effettuato da apposita icona presente sul menu START);
    b. Comunicare l'accaduto ai Sistemi Informativi dell'organizzazione, 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.
18) Nel caso l'utilizzatore sbagli per più di 5 volte l'inserimento della password di accesso alla rete, l'account è automaticamente disabilitato per 1 ora; la riabilitazione dell'account è automatica eventualmente anticipabile tramite richiesta al supporto tecnico. È anche possibile utilizzare il sistema di *self-service password*.
19) In caso di prolungato inutilizzo dell'account (per più di 6 mesi), in caso di cessazione o trasferimento degli utilizzatori, la procedura di verifica nell'ambito delle autorizzazioni ne comporterà la disabilitazione. L'eventuale riabilitazione dovrà essere autorizzata dal soggetto designato.
20) Nei casi di particolare emergenza oppure in presenza di comportamenti che possano generare problemi di sicurezza, il personale dei sistemi informativi è autorizzato alla momentanea disattivazione degli account e all'isolamento dei sistemi utilizzati. Risolta la problematica evidenziata sarà cura del personale dei sistemi informativi ripristinare le precedenti autorizzazioni.

21) I sistemi informativi non inviano mai tramite e-mail richieste di cambiamento o reset password dell'account di accesso ai sistemi dell'organizzazione. Pertanto, eventuali e-mail che richiedano tramite *link* la modifica della password devono essere marcate come spam e cestinate.
22) Non è consentito memorizzare account di accesso ai sistemi e servizi dell'organizzazione in documenti salvati in sistemi o dispositivi al di fuori del perimetro dell'organizzazione e ad accesso pubblico, inclusi sistemi di file hosting.
23) Gli account di amministratore 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.

Art. 12. - Posta elettronica convenzionale

1) La posta elettronica è uno strumento di comunicazione e deve essere utilizzato soltanto per effettuare corrispondenze legate al servizio svolto nell'organizzazione, anche nel caso di account di posta elettronica di tipo nominativo. In nessun caso sono previsti indirizzi di posta elettronica ad uso privato dell'utilizzatore.
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 sull'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, l'età, la vita sessuale 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 proprio diretto superiore.
4) La posta elettronica ordinaria o e-mail secondo la recente giurisprudenza[1] e 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[2], è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
5) Un messaggio di posta elettronica convenzionale inviato allo stesso dominio (@inrca.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 e in particolare il contenuto della comunicazione (testo e allegati).
6) Alla conclusione della sessione di lavoro effettuare sempre la disconnessione (Log out) dal sistema di posta utilizzato.
7) L'indirizzo di posta elettronica non deve essere utilizzato per la registrazione a siti web che non siano in qualche modo legati alle attività svolte dagli utilizzatori intestatari dell'account anche al fine di limitare lo spam.
8) Non lanciare mai i link di annullamento alle sottoscrizioni delle e-mail considerate indesiderate (il cd. "*unsubscribe*").
9) 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:

[1] Sentenze n. 14716/2011 e n. 11402/2016 Tribunale di Milano
[2] 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 marcare come spam "service145@mail.145.com";
b. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiono a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo *phishing*; posizionare 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 stile Google), 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.

10) Nei casi dubbi non aprire e-mail o contenuti e contattare il supporto tecnico che provvederà alla verifica.
11) La configurazione del client della posta aziendale sui dispositivi mobili di tipo personale (es. smartphone e tablet) è permesso a patto di adottare alcune misure di sicurezza:
    a. Pin di accesso o combinazione di sblocco o impronta
    b. Lock automatico dello schermo
    c. Aggiornamento costante del sistema operativo del dispositivo in uso
    d. Wipe out prima dello smaltimento o cessione.
12) L'utilizzo di *forward* automatico di posta dell'organizzazione su altri sistemi (es. Gmail) non è consentito al fine di garantire un adeguato livello di sicurezza dei contenuti dei messaggi (es. allegati contenti 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).
13) La posta elettronica fornita dall'organizzazione non può essere utilizzata per scopi personali estranei all'attività lavorativa. Viceversa, non è consentito utilizzare o fornire e-mail personali per scambiare informazioni, contenuti o allegati connesse all'attività lavorativa.
14) L'invio di file con contenuti sensibili per l'organizzazione tramite link ai sistemi di file hosting, specie se di tipo gratuito, è permesso solo se i file sono criptati e le chiavi di criptazione sono condivise su altro media.
15) È fortemente consigliato non consultare la posta elettronica dell'organizzazione presso Internet point, WiFi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar).
16) Le raccomandazioni o indicazioni, estranee all'ambito lavorativo, inviate via e-mail non devono essere seguite poiché nella maggior parte dei casi si tratta di virus HOAX (bufale) (es. "cancella questo file sul tuo computer", "gira questa email a tutti i tuoi amici"). In caso di dubbi contattare il supporto tecnico.
17) 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 grossi guadagni in cambio di somme di denaro da anticipare).
18) 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.
19) Non attivare mai i link presenti nelle cosiddette e-mail di reset della password.
20) Non rispondere e inoltrare e-mail delle cosiddette catene di Sant'Antonio o rispondere alle e-mail di spam.
21) Le policy della posta elettronica prevedono le seguenti limitazioni:
    a. Dimensione massima della casella di posta utente pari a massimo 10 GB (evitare di trasformare il sistema di posta elettronica in sistema di archiviazione);
    b. Dimensione massima degli allegati inviati o ricevuti pari a 30 MB;
    c. Limite massimo di destinatari contemporanei pari a 100;

d. Tempo di conservazione dei messaggi cancellati pari a 3 mesi;

22) In caso di invio al di fuori del dominio di posta dell'organizzazione gli allegati inviati via e-mail contenenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (es. via telefono).
23) Le e-mail contenenti presunte evidenze di reati relativi alla sicurezza informatica devono essere prima visionate dal personale tecnico e poi, se del caso, informate le autorità per la presentazione della denuncia; questo al fine di evitare falsi allarmi.
24) Nel caso si riceva una e-mail da un collega visibilmente contraffatta, informare immediatamente il supporto tecnico.
25) Nel caso la marcatura come spam di un insieme ricorrente di messaggi non riduca il problema, è possibile attivare i cosiddetti filtri personalizzati, in grado di marcare automaticamente tipologie di e-mail indesiderate.
26) Al fine di contenere lo spazio di memoria del server di posta, in conformità ai principi di minimizzazione dei dati (art. 5, par. 1, lett. c GDPR) e di limitazione della conservazione (art. 5, par. 1, lett. e) GDPR) l'utilizzatore del servizio di posta elettronica provvede alla periodica cancellazione delle e-mail non rilevanti per la propria attività lavorativa.
27) Nel caso di comportamenti anomali del personal computer a seguito dell'apertura di una e-mail, è necessario:
    a. Staccare immediatamente il cavo di rete;
    b. Lasciare il computer accesso per successive verifiche dei tecnici;
    c. Segnalare immediatamente l'accaduto al supporto tecnico e al proprio Dirigente.
28) La politica di sicurezza dell'organizzazione prevede la disabilitazione dell'account di posta elettronica coerentemente con la disabilitazione dell'account utente; eventuali eccezioni dovranno essere autorizzate dal soggetto designato.
29) La politica di conservazione della posta elettronica prevede un tempo massimo di *retention* per la casella postale di 3 mesi dopo la cessazione del rapporto di lavoro; eventuali eccezioni sui tempi di conservazione, la re-direzione della nuova posta su altro indirizzo sempre di Istituto dovranno essere autorizzate dal soggetto designato.
30) La politica di sicurezza dell'organizzazione, anche in ottica di lavoro in mobilità, prevede in via esclusiva il client di posta elettronica basato sul web denominato "Outlook sul web" e il client in ambito *mobile* permesso sui soli dispositivi di proprietà dell'organizzazione.
31) La mappatura, anche se in sola lettura, dei file di archiviazione con estensione "PST" non è consentita. Eventuali malfunzionamenti o perdite di dati dovute a questa "cattiva pratica" saranno imputate in termini di responsabilità e maggiori costi al singolo utilizzatore.
32) I sistemi di posta elettronica convenzionale non consentono di assicurare le dovute caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. Per tale motivazione la conservazione dei documenti necessari per l'ordinario svolgimento e la continuità delle attività deve essere assicurata utilizzando gli specifici sistemi di gestione documentale, individuando i documenti che nel corso dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche.

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 esente da rischi. Per questo motivo valgono le stesse regole e indicazioni fornite per la posta elettronica convenzionale sia per quanto concernente la sicurezza che la protezione dei dati personali.

Art. 14. - Firma elettronica

1) Le Firme Elettroniche, ai sensi del Regolamento UE n. 910/2014 (eIDAS, *Electronic IDentification Authentication and Signature*) e del Codice dell'Amministrazione Digitale 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 Qualsiasi autenticazione a piattaforma con credenziali (utente e password)	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. (art.21)
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. (art.21)
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. (art.21)

2) L'utilizzatore dotato di strumenti di firma è responsabile della conservazione in sicurezza di tutte le componenti (hardware come ad esempio la Smart card, PIN e Password). La perdita degli strumenti di firma o di semplice sospetto della perdita di segretezza della password o del PIN, deve essere immediatamente comunicata al supporto tecnico e al DPO.
3) È fondamentale conservare separati i dispositivi di firma (Smart card o Token) dal PIN e dalla password (preferibile ricordare e non conservare le credenziali).

4) La firma di atti o documenti dell'organizzazione è responsabilità diretta dell'intestatario della firma elettronica (di qualsiasi tipologia sopra riportata).
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 preferibilmente in formato PDF, PDF/A (progettato per la conservazione dei documenti amministrativi) o XML.
7) Le tipologie di firme accettate sono P7M (CAeDES), PDF (PAeDES) e XML (XADeS) . Altri formati non sono accettati dall'organizzazione o dalle piattaforme di conservazione.
8) Le regole per le password all'art. 11 sono valide anche nella definizione della password e PIN/PUK di firma.
9) Nel caso il software di verifica delle firme segnali delle anomalie è necessario:
    a. Verificare che la lista delle CA sia aggiornata;
    b. Verificare il firmatario;
    c. Eventualmente richiedere di nuovo il documento firmato al firmatario.
10) La conservazione sostitutiva dei documenti firmati digitalmente segue quanto previsto dalla regolamentazione in materia.

Art. 15. - Instant messaging

1) Gli strumenti di comunicazione sincrona permettono facili e immediate comunicazioni 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 WiFi e l'utilizzo di un dispositivo mobile. Le piattaforme più diffuse sono WeChat, Facebook Messenger e WhatsApp. L'utilizzo di questi strumenti in ambito lavorativo è consentito per le sole comunicazioni interpersonali di servizio (fissare un appuntamento, auguri, ecc.).
2) L'invio o la condivisione attraverso le piattaforme social o di instant messaging di documenti, immagini o video con evidenza di dati personali trattati dall'Istituto non è permesso. Nel caso di impellenza o necessità di utilizzo di questa tipologia di strumenti è opportuno adottare le normali tecniche di anonimizzazione dei soggetti interessati ovvero cancellare con il bianchetto prima dell'acquisizione, offuscare parte dell'immagine prima dell'invio, adottare tecniche di *crop, pixelling* o sfocatura.
3) Eventuali condivisioni improprie di dati personali attraverso piattaforme social o di instant messaging sarà ricondotta in termini di responsabilità all'utilizzatore mittente.
4) La condivisione di dati personali o di informazioni riservate relative all'ambito lavorativo su piattaforme di messaggistica non risulta conforme per le seguenti motivazioni:
    a. I dati sono inviati in server posizionati in paesi Extra UE senza quanto previsto 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 indicizzati;
    c. Tutti gli utenti sono profilati;
    d. Non è al momento prevedibile cosa sarà dei dati inviati né quali potranno essere gli impatti sugli interessati;
    e. Il backup di WhatsApp (famiglia Facebook) sui sistemi basati su sistema operativo Android non sono criptati quando sono salvati su Google Drive;
    f. Le impostazioni di sicurezza dei dispositivi mobile non garantiscono un adeguato livello di protezione dei dati.
5) Eventuali messaggi arrivati su dispositivi mobile contenenti dati personali o informazioni riservate legate all'ambito lavorativo devono essere cancellate.
6) Verificare periodicamente le impostazioni relative alle autorizzazioni delle applicazioni dei dispositivi mobile e le relative impostazioni sulla privacy (cosiddetto "privacy setting").

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. - Sistemi informatici

1) I sistemi informatici sono installati presso le singole postazioni di lavoro (client) o presso i datacenter (server) soltanto dopo:
    a. Aggiornamento di tutte le componenti software (firmware, sistema operativo, middleware e componenti);
    b. Installazione delle componenti obbligatorie (come agent e antivirus);
    c. Verifica tramite procedura di *Vulnerability assessment* senza evidenze rispetto ad elementi elevati (HIGH) o critici (WARNING);
    d. Redazione della necessaria documentazione sul sistema e sulle eventuali modalità di re-installazione e ripristino;
    e. Aver testato le funzionalità base ed aver redatto il documento di omologazione (check-list).
2) Il collegamento di sistemi o dispositivi non conformi a quanto riportato al comma 1), ad esempio per vincoli tecnici o di compatibilità, può avvenire in via esclusiva su specifica sottorete, separata e posta in sicurezza rispetto alla rete dell'organizzazione.

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

1) I cosiddetti BYOD (Bring Your Own Device, letteralmente "porta il tuo dispositivo"):
    a. possono essere utilizzati soltanto come sistemi isolati non collegati alla rete dell'organizzazione;
    b. connessi al Wi-Fi aziendale con accesso di tipo *guest* (se presente);
    c. connessi tramite vpn (vedi articolo "accesso remoto (vpn)").
2) Non è consentito il collegamento alla rete dell'organizzazione di sistemi o dispositivi non distribuiti ufficialmente dal SIA. A chiunque effettui il collegamento diretto alla rete dell'organizzazione (sono esclusi i Wi-Fi pubblici) di sistemi o dispositivi saranno addebitati eventuali costi di rispristino o ulteriori danni che dovessero originarsi da un collegamento non autorizzato.
3) Eventuali sistemi o dispositivi non autorizzati collegati alla rete dell'organizzazione saranno considerati come attacco al sistema informatico e segnalati al DPO e, nei casi più gravi, all'autorità giudiziaria
4) 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.
5) In conformità alla normativa vigente in tema di protezione dei dati personali è sconsigliato salvare sui BYOD i dati personali, specialmente se di natura particolare, raccolti durante le attività lavorative. È comunque permesso il salvataggio temporaneo dei file e documenti di lavoro sulla postazione di proprietà personale a patto di provvedere, una volta effettuata la redazione o l'elaborazione, alla completa eliminazione o, in alternativa, al salvataggio in formato criptato protetto da chiave, secondo procedura differenziata per file di tipo .docx, .xlsx, .accdb (direttamente integrato nell'applicativo di produttività individuale) e per altre tipologie di file che richiedono invece l'utilizzo di strumenti esterni.
6) Il trasporto al di fuori del perimetro aziendale di dispositivi di memorizzazione contenenti dati sensibili non è consentito. 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 (owner del dispositivo).
7) Nell'ipotesi di smarrimento o furto di un dispositivo personale contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, l'utilizzatore è tenuto a comunicare al DPO l'accaduto per l'attivazione della procedura di data breach.

Art. 18. - Utilizzo di postazioni di lavoro e dispositivi di proprietà dell'organizzazione

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 sia comprometterne il funzionamento che, in casi particolari, 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) Non è consentito modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete aziendale e alla alimentazione elettrica, da parte dell'utilizzatore o di personale esterno, senza specifica autorizzazione del personale del servizio di supporto tecnico SIA.
3) Non è consentito l'uso di software applicativi diversi da quelli distribuiti 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).
4) Non è consentito conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, e-mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.
5) 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.
6) L'utilizzatore di sistemi e servizi IT è invitato alla immediata segnalazione al servizio di supporto tecnico in caso di danni o funzionalità parziale dei dispositivi o delle apparecchiature.
7) Eventuali specifiche indicazione o istruzioni fornite dal personale di supporto tecnico devono essere rispettate.
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 applicativi attivi, e infine del sistema (Windows-l (elle), oppure Start – Arresta / Disconnetti).
9) 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 per l'attivazione della procedura di data *breach* e, a seguire, al supporto tecnico dell'organizzazione per l'attivazione delle previste procedure di sicurezza (*device wipe-out*).
10) Nel caso di utilizzo di dispositivi di proprietà dell'Istituto al di fuori del perimetro di sicurezza è necessario eliminare i file contenti dati di tipo particolare o procedere con la criptazione a livello disco, cartella o singolo file. È comunque permesso il salvataggio temporaneo dei file e documenti di lavoro sulla postazione di proprietà personale a patto di provvedere, una volta effettuata la redazione o l'elaborazione, alla completa eliminazione o, in alternativa, al salvataggio in formato criptato protetto da chiave, secondo procedura differenziata per file di tipo .docx, .xlsx, .accdb (direttamente integrato nell'applicativo di produttività individuale) e per altre tipologie di file che richiedono invece l'utilizzo di strumenti esterni. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori del perimetro dell'organizzazione, sarà attribuita all'utilizzatore assegnatario.

Art. 19. - Utilizzo delle cartelle collegate e condivise

1) Le informazioni costituiscono un patrimonio per l'organizzazione, costituito da informazioni:
    a. strutturate, gestite attraverso applicazioni software verticali e motori di database;
    b. non strutturate, gestite attraverso strumenti di produttività individuale (come MS-Office e Libre/OpenOffice).

La protezione delle informazioni strutturate è in carico ai Sistemi informativi dell'organizzazione; per quanto riguarda le informazioni non strutturate permane in carico ai Sistemi informativi la sola protezione dei dati conservati nelle condivisioni di rete, messe a disposizione degli utilizzatori. I dati salvati nelle unità locali dei sistemi o nei dispositivi mobili non sono né protetti, né proteggibili dalle procedure previste.

Le tecnologie implementate nei sistemi di storage per le unità di rete garantiscono un livello nettamente superiore di sicurezza grazie, ad esempio, alla gestione del *versioning* dei file (cd. *shadowing*); la memorizzazione file rilevanti per l'organizzazione deve sempre avvenire nelle unità di rete, le uniche a garantire un adeguato livello di sicurezza.

2) La riservatezza dei dati, specie se personali, è garantita dalle tecnologie di gestione degli accessi che permettono una definizione granulare dei permessi, gestiti preferibilmente per gruppo di appartenenza. Per tale motivo è necessario da parte del soggetto designato o comunque responsabile di UOS/UOC procedere con la definizione del proprio albero di cartelle e relative autorizzazioni. In assenza di istruzioni specifiche valgono le impostazioni di *default* che prevedono il solo accesso del personale dirigente e designato.
3) Tutte le unità disco, di tipo locale o di rete, non sono a disponibilità infinita. Per questo motivo sono imposte delle quote di utilizzo.
4) Le cartelle di rete collegate e condivise sono di 4 tipi:
    a. Cartella ad accesso personale dove salvare i documenti ancora in lavorazione o non ancora da condividere;
    b. Cartella ad uso Unità Operativa per la condivisione delle informazioni tra i componenti dello stesso gruppo di lavoro / ufficio;
    c. Sistema di file hosting per la condivisione via web;
    d. Cartella di progetto ad uso combinato tra più Unità Operative per la condivisione interdipartimentale.
5) Gli utilizzatori, all'atto dell'attivazione dell'account di accesso alla rete aziendale, possono richiedere l'attivazione sono dell'unità di tipo personale. Le altre unità devono essere richieste dal referente del progetto o dal dirigente responsabile di una delle Unità Operative coinvolte.
6) Nelle cartelle condivise (es. ad uso UO) è possibile impostare stratificazioni dei permessi, per il solo primo livello di cartelle (es. un gruppo di utenti legge mentre altri possono anche scrivere su una o più cartelle, mentre il resto delle informazioni risulta ad accesso libero tra gli autorizzati).
7) Le cartelle condivise sono replicate in sicurezza (backup) tutti i giorni; è garantita una *retention* (tempo massimo di conservazione delle versioni precedenti delle copie) di 1 settimana; sono disponibili diverse livelli di replica al fine da garantire maggiori possibilità di recupero.
8) Non è consentito conservare file protetti dal diritto d'autore nelle cartelle condivise.
9) I marchi, i segreti commerciali o i diritti di brevetto devono essere conservati con particolari accortezze e ad accesso ristretto.
10) Nella cartella di UO gli utilizzatori possono creare a piacimento altre cartelle che per impostazioni predefinita sono accessibili a tutti gli appartenenti alla UO. La configurazione e le eventuali variazioni dei permessi sulle singole cartelle devono essere comunicate al supporto tecnico per le necessarie impostazioni. Nel caso di progetto condiviso tra più UO è necessario procedere con la richiesta di una Cartella progetto posizionata nel disco condiviso.
11) Gli utilizzatori hanno comunque il compito di:
    a. contenere lo spazio disco occupato entro le quote assegnate;
    b. mantenere le cartelle in ordine, con particolare riguardo alle cartelle condivise, cercando di non stratificare le cartelle oltre il terzo livello (es. cartella\sottocartella1\sottocartella2);
    c. eliminare i file non più utilizzati o duplicati (es. file1.vers1, file1.vers2, file1.bak, file1.old);

d. evitare la duplicazione delle informazioni già contenute in applicativi specifici aziendali (export dei dati per successiva elaborazione su Excel) anche in considerazione degli obblighi in tema di protezione dati personali.

Art. 20. - File hosting

1) È possibile utilizzare il sistemi aziendale di condivisione disponibile all'indirizzo https://cloud.inrca.it
2) Il file hosting di dati personali e riservati su piattaforme gratuite non è consentito a meno di criptazione con invio delle chiavi su altro canale.

Art. 21. - Navigazione Internet

1) Internet è la fonte di informazioni più vasta esistente, quindi irrinunciabile tanto per il personale operativo quanto per il personale amministrativo. L'interoperabilità tra enti pubblici passa sia attraverso il Sistema Pubblico di Connettività sia su 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, non è consentito in tutti i siti web appartenenti alle categorie previste nell'Appendice *Content Filtering Rating Categories*, navigare per fini ludici o personali, effettuare upload o download di file e documenti non connessi all'attività lavorativa, effettuare streaming audio o video (es. radio o tv via Internet), effettuare chat on-line.
3) Non è consentita 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) Non è consentito navigare in siti web che possano comportare nei sistemi deputati alla connettività, al monitoraggio e alla protezione della connessione Internet, trattamenti involontari di dati personali di tipo sensibile (esempio convinzioni religiose, politiche, stato di salute, vita sessuale) riconducibili agli utilizzatori del servizio.
5) Considerati i rischi connessi con la navigazione web, relativi al singolo computer e potenzialmente a tutto il patrimonio informativo aziendale, con evidenti problemi di continuità dei servizi e di immagine, nonostante tutte le protezioni attivate, è sempre in capo al singolo utilizzatore la verifica ultima di:
    a. **Sito web**: verificare 2 volte l'indirizzo completo (attenzione ai siti web che appaiono simili ma non lo sono: www.inrrca.it o www.inrca.<sitostrano>.it);
    b. **Certificato**: evitare i siti non sicuri (http) e nel caso di siti in https verificare che il certificato riporti esattamente l'intestatario del sito web in questione;
    c. **Riferimenti**: i siti dei cosiddetti *scammer* non hanno indirizzo o telefoni
    d. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiono a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo *phishing*; posizionare il cursore del mouse sul link per visualizzare la reale destinazione (ad esempio evitare di fare click su link, ad esempio www.inrca.it con destinazione www.inrca.ru);
    e. **Download**: evitare di scaricare da siti non ufficiali/istituzionali documenti, software o app, componenti aggiuntivi (plug-in del browser o componenti "dinamici" come ActiveX o funzioni JavaScript);
    f. **Contenuti**: per riconoscere siti non ufficiali a volte è sufficiente verificare grossolani errori sintattici (es. traduzione automatiche);

g. **Verifiche web**: attraverso i motori di ricerca è possibile trovare altre informazioni sul sito web.

Nei casi dubbi non aprire il sito web, chiudere il browser e, nel caso il sistema inizi ad avere comportamenti singolari, contattare il supporto tecnico che provvederà alla verifica secondo le procedure di sicurezza.

6) I rischi derivanti dall'utilizzo delle informazioni personali o delle carte di credito nei sistemi e nella rete dell'organizzazione sono sempre in capo all'utilizzatore. INRCA non è responsabile per eventuali perdite di riservatezza delle informazioni personali o per altri danni.
7) 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.
8) 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.
9) La trasmissione di informazioni proprietarie, riservate o altrimenti sensibili, contenenti dati personali di tipo particolare non è consentita a meno dell'adozione di specifici controlli e protezioni.
10) La larghezza di banda della rete locale (interna) e la connessione Internet sono risorse condivise e limitate. Utilizzi indebiti di un singolo potrebbero impattare sulle attività degli altri utilizzatori. Per questo motivo i sistemi informativi possono adottare delle politiche di gestione della banda in funzione delle stabilite priorità (*Traffic* o *Packet shaping*).
11) Le attività degli utilizzatori sono monitorate da un sistema automatico che verifica:
    a. la quantità di dati scaricati giornalmente e mensilmente;
    b. le tipologie di siti visitati (in vista aggregata e conformi alle politiche di *Content filtering*);
    c. le tempistiche totali di navigazione.

    I comportamenti degli utilizzatori non conformi ai parametri generali sopra riportati e quindi non corretti possono comportare la disabilitazione dell'account per motivi di sicurezza o continuità operativa (a meno di specifica autorizzazione).
12) 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 (attivata la cd. rotazione dei log file). La conservazione dei file di registrazione della navigazione degli utilizzatori è limitata a 7 giorni, che è considerato il periodo strettamente necessario per il perseguimento delle finalità di sicurezza dell'Istituto, fatti salvi in ogni caso specifici obblighi di legge.

Art. 22. - Reti locali (LAN), reti metropolitane (MAN) e reti geografiche (WAN)

1) Le infrastrutture di rete di tipo locale (LAN), le reti di tipo metropolitano (MAN) o geografico (WAN, come ad esempio la tecnologia denominata MPLS utilizzata in istituto) permettono il collegamento e la condivisione delle informazioni tra tutti i sistemi e i dispositivi collegati. In considerazione dell'architettura progettata per la massima libertà di esercizio, il reale livello di sicurezza è equiparabile al cosiddetto "anello più debole". Per quanto premesso è necessario garantire il massimo livello di sicurezza su tutti i sistemi e dispositivi collegati alla rete di istituto.

2) Non è consentito collegare alla rete locale di istituto sistemi, dispositivi o apparati di qualsiasi natura che non siano stati:
    a. verificati anche dal punto di vista di eventuali vulnerabilità, autorizzati dal SIA, registrati nell'asset management in uso.
3) Il collegamento di sistemi, dispositivi o apparati alla rete di istituto se effettuata in assenza di tutti i requisiti sopra indicati sarà ricondotta in termini di responsabilità ai singoli direttori di UOC/UOS.

Art. 23. - Utilizzo Reti Wi-Fi pubbliche

1) Le reti Wi-Fi pubbliche con l'opzione di protezione di tipo WEP non possono essere utilizzate per ragioni di sicurezza, in considerazione del livello di riservatezza garantito. Utilizzare soltanto reti Wi-Fi che implementano protocolli di tipo WPA o WPA2 (verificare nelle impostazioni del Wi-Fi).
2) Per ragioni di sicurezza, si può utilizzare la connessione Wi-Fi pubblica solo per effettuare navigazione informativa, ma non per accedere alle piattaforme aziendali. In caso di necessità optare per una connessione di tipo *Tethering* ovvero utilizzando il proprio smartphone come gateway Internet.

Art. 24. - Utilizzo Reti Bluetooth

1) Il Bluetooth deve essere attivato soltanto quando necessario; alla fine della sessione di lavoro deve essere disattivato.
2) L'ambiente circostante deve essere sicuro quindi devono essere evitati luoghi pubblici (con potenziale promiscuità inferiore ai 50 metri).
3) La visibilità del dispositivo via protocollo Bluetooth deve essere attivata solo se necessario.
4) Attivare sempre le opzioni di sicurezza come autenticazione e cifratura delle comunicazioni.

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 ma in forme tali da precludere la possibilità di identificazione dei soggetti. 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 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 tesa 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.
4) I sistemi di sicurezza sono configurati in modo da prevenire e bloccare operazioni considerate potenzialmente pericolose oppure non direttamente correlate all'attività lavorativa, quali l'upload e/o il download di file o software aventi particolari caratteristiche, ad esempio dimensionali o di tipologia di contenuti; eventuali eccezioni dovranno essere segnalate ai Sistemi Informativi.
5) L'utilizzatore di sistemi e servizi IT non deve modificare, aggirare, disabilitare i controlli di sicurezza. Eventuali attività ritenute sospette comporteranno l'immediata disabilitazione 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).

6) 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.
7) I sistemi o i dispositivi compromessi a seguito di attacco devono essere ripristinati dal personale dei Sistemi Informativi seguendo le procedure previste.
8) 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 agli specifici aggiornamenti.

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; altra modalità più subdola è cercare di stabilire un certo livello di fiducia in modo che la vittima riveli informazioni riservate. Per questo motivo non è consentito:
    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.

Art. 27. - Accesso remoto (VPN)

1) L'acceso dall'esterno alla rete aziendale può avvenire soltanto in tre modi:
    a. Utilizzando le piattaforme esposte sul web (es. Posta elettronica, Sito web, ecc.);
    b. Virtual Private Network (VPN): client o Web;
    c. LAN-to-LAN IPsec Tunnel.
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, non sono fornite VPN ad accesso completo di tutta la rete dell'organizzazione.
3) L'autorizzazione deve essere rinnovata di anno in anno sempre attraverso la procedura di abilitazione o, in alternativa, è possibile procedere con la verifica periodica dell'ambito di autorizzazione di ciascun utilizzatore. Gli account VPN non rinnovati sono automaticamente disabilitati alla fine del periodo.
4) La modalità predefinita è la Vpn web, in casi del tutto particolari qualora sia tecnicamente necessario l'utilizzo del client Vpn, la macchina su cui installare detto client deve essere:
    a. Protetta da password di una certa complessità;
    b. Esente da applicativi software non licenziati o crack di sblocco;
    c. Aggiornata all'ultima versione disponibile di sistema operativo (i sistemi operativi in *out of support* devono essere dotati di sistema di *virtual patching*);
    d. Dotata di software antivirus, con basi aggiornate 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 le credenziali di accesso dai sistemi informativi.
6) Gli utilizzatori delle connessioni VPN, dato che sono essenzialmente estensioni della rete dell'organizzazione, devono sottostare in tutto e per tutto al presente regolamento.
7) I comportamenti non conformi o anche solamente sospetti negli accessi o durante le sessioni comporteranno la disabilitazione dell'account di connessione VPN.
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 dei componenti da fonti affidabili e perfettamente licenziati.

Art. 28. - Erogazione del servizio di Supporto tecnico (Service Operation)

1) L'erogazione del servizio di supporto tecnico è basato su risorse e priorità. Questo perché le risorse non sono infinite ed è necessario trovare un equilibrio tra costi e affidabilità del servizio, con specifico riferimento ai tempi di risposta, possibilmente rientrando nei livelli di servizio concordati (SLA).
2) La priorità si basa sulla criticità dei servizi:
   sistemi e servizi critici, front-office, gestione emergenze;
   sistemi e servizi secondari (es. amministrazione);
   sistemi e servizi con problematiche non bloccanti.
3) Ad ogni richiesta di intervento è associato un ticket, consultabile dal personale tecnico e dagli utilizzatori richiedenti. Il ticket è preso in carico dal singolo tecnico, specialista nella tipologia di intervento richiesto. Il ticket può essere chiuso dal tecnico che prende in carico l'intervento nel caso non si evidenzino le problematiche segnalate dall'utilizzatore o al momento della risoluzione.
4) Nel caso il problema si ripresenti, l'utilizzatore deve riaprire un secondo ticket, facendo riferimento al fatto di aver già segnalato il problema.
5) Le attività del personale dei sistemi informativi sono sempre legate ad un ticket. Non è possibile richiedere servizi senza una richiesta di intervento effettuata tramite il sistema di help desk disponibile nella intranet aziendale alla voce "Infotic Ticketing assistenza informatica"
6) La richiesta è importante sia per il tracciamento delle attività, al fine di garantire le dovute priorità come anche permettere la misurazione delle performance del personale impiegato nel servizio.
7) Il personale tecnico ha facoltà di accesso ai dispositivi e alle informazioni essendo stato nominato Amministratore di Sistema. L'accesso può avvenire con proprie credenziali o tramite sessioni di controllo remoto, avendo cura di non acquisire per nessun motivo informazioni riservate, personali o particolari.

Art. 29. - 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 sulla sicurezza.
3) I Sistemi Informativi, al fine di migliorare il livello di sicurezza, organizzano con cadenza 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. 30. - Utilizzatore dei servizi e degli applicativi

1) L'Utilizzatore dei servizi e degli applicativi è un individuo espressamente autorizzato a 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 o all'Amministratore di Sistema applicativo 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, illustrate durante le sessioni formative o comunicate durante il *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. 31. - Dirigenti di UOS/UOC/Dipartimenti

1) Il dirigente di Unità Operativa, in forza della nomina a soggetto Designato del trattamento dei dati personali, provvede all'autorizzazione degli utilizzatori (autorizzati al trattamento dei dati personali) 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 all'assistenza tecnica eventuali 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. 32. - 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 Unità Operativa che provvede ad attribuire singolarmente l'ambito di autorizzazione.
2) 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. Effettuare controlli tecnici a tutti i livelli della catena tecnologica per verificare funzionalità e sicurezza di singoli sistemi, dispositivi e applicazioni software, secondo le modalità previste dalle procedure interne;

k. Operare secondo le prescrizioni di sicurezza e le procedure interne previste.

3) Sono considerati Amministratori di Sistema anche i soggetti che gestiscono i profili di autorizzazione applicativa i cui compiti sono quindi relativi a tale attività.

Art. 33. - Fornitori di prodotti e servizi

1) I fornitori di prodotti e servizi IT dell'Istituto 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 a un applicativo, il personale tecnico è nominato Amministratore di Sistema dal titolare dell'azienda appaltatrice.

CAPO V – Prescrizioni per gli utilizzatori

Art. 34. - Gestione di una conference call (*Etiquette Rules*)

1) In una riunione tramite strumenti informatici valgono le stesse regole di educazione di una riunione convenzionale frontale. Vi sono però dei vincoli e dei possibili problemi legati alle tecnologie che richiedono una particolare attenzione al fine di evitare perdite di tempo e insoddisfazione dei partecipanti.
2) È importante concordare con congruo anticipo lo strumento e il momento preciso in cui tenere la call. L'organizzatore deve inviare un invito, verificando prima le agende condivise, in modo che sia possibile attivare semplicemente con un click lo strumento prescelto per la conferenza, senza sprechi di tempo e chiamate parallele del tipo "cosa utilizziamo per la call?";
3) La regola generale prescrive che chi ha bisogno cerca, invita e chiama; viceversa, chi fornisce il supporto deve essere chiamato da colui che ha bisogno;
4) Considerati gli strumenti, le modalità e gli immancabili disturbi e disconnessioni, la call dovrebbe essere di una durata pari a 10, 20 o al massimo di 30 minuti nei quali concentrare l'essenza dei contenuti della riunione. I materiali dovrebbero essere condivisi con congruo anticipo in modo che i partecipanti possano comunque apportare il loro contributo senza discussioni o perdite di tempo; le slide per le presentazioni non dovrebbero essere condivise preliminarmente ma mostrate esclusivamente nella sessione;
5) Nel caso in cui un partecipante sappia in anticipo di un probabile ritardo, è tenuto a comunicarlo all'organizzatore in modo che, se possibile, la call venga fissata in un secondo momento o posticipata;
6) Data l'impossibilità di multitasking nelle call, quando un partecipante non risponde alle chiamate o agli inviti, non è corretto insistere o lasciare messaggi, almeno la prima volta. Se dopo diversi tentativi il soggetto non risponde, è opportuno lasciare un messaggio o inviare una e-mail. A meno di particolari urgenze, l'organizzatore non dovrebbe richiamare;
7) L'organizzatore dovrebbe invitare alla call il minor numero di persone possibile poiché più persone partecipano, più difficilmente verrà prestata la dovuta attenzione;
8) Tutti i partecipanti alla call devono prestare attenzione al luogo da dove viene effettuata la chiamata, ovvero in ambiente tranquillo, senza rumori di fondo e sempre supportati da una buona connettività (di solito il Wi-Fi in giardino non permette lo stesso livello di qualità audio e video); sono esclusi luoghi pubblici, in presenza di altre persone anche se familiari, specie nel caso di trattazione di temi dell'organizzazione, delicati o comunque sottoposti a segreto di ufficio;
9) Ad esclusione dell'organizzatore, tutti i partecipanti si accertano di tenere chiusa (in modalità mute) la comunicazione audio in modo da evitare rumori di fondo o effetti Larsen (feedback acustico o più ritorno); il passaggio da muto a microfono attivo è effettuato dal partecipante solo in caso di richiesta di intervento o per richiedere la parola;

10) In caso di utilizzo di sistemi di comunicazione nuovi, non conosciuti, è opportuno accertarsi preliminarmente dei prerequisiti (installazione di applicazioni software, componenti, plug-in, livelli audio) ed effettuare almeno un test preliminare;
11) Nelle prime sessioni di conference è preferibile utilizzare la versione video con la ripresa delle persone sfruttando la possibilità di conoscersi se non se ne è avuta in precedenza occasione; per le versioni successive può essere consigliata la audio conference (senza video) con condivisione dei materiali;
12) A meno di particolari situazioni, la call deve iniziare e concludersi nei tempi stabiliti; non è corretto attendere indefinitamente i ritardatari soprattutto per non incoraggiare la loro condotta, pertanto, chi arriva in ritardo potrà essere contattato direttamente dall'organizzatore in modo da poter ricevere le informazioni perdute senza effetti negativi sugli altri partecipanti;
13) L'organizzatore della call deve mostrarsi immediatamente, presentare i partecipanti, esporre i contenuti e dare le dovute indicazioni di servizio, tra le quali il tempo previsto per la call ed i relativi interventi; i partecipanti devono venire a conoscenza sin da subito di ciò che l'organizzatore si aspetta da loro;
14) La modalità di comunicazione frontale e in call si differenzia altresì per la necessità di adottare un linguaggio più semplice, frasi concise e pause regolari tra i differenti contenuti. Questo consentirà ai partecipanti di passare oltre o in alternativa di porre delle congrue domande;
15) L'organizzatore della call deve prestare attenzione alla stessa partecipazione, intervenendo e togliendo la parola a chi prova a monopolizzare la sessione e chiamando gli altri ad intervenire;
16) Pur avendo a disposizione altri strumenti del sistema informatico o lo smartphone, non è corretto continuare a rispondere alle e-mail o ai messaggi mentre gli altri partecipano attivamente alla sessione; le altre attività devono essere posticipate dopo la call;
17) Prima della fine della sessione è necessario avvertire i partecipanti della imminente conclusione e della possibilità da quel momento di rivolgere opportune domande;
18) L'organizzatore della call, o un soggetto nominato segretario, deve annotare ed in seguito condividere il report della sessione:
    a. Motivo della call / obiettivi
    b. Nominativo e ruolo partecipanti
    c. Argomenti discussi e relativi interventi
    d. Risultanze

CAPO VI – Gestione eventi ed emergenze

Art. 35. - 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. 36. - 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) Il personale di supporto di primo livello, una volta identificato l'incidente, allerta immediatamente il personale di supporto di secondo livello, composto 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.
3) Il supporto di secondo livello 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).
4) Una volta risolte le cause dell'incidente e riportato alla normalità il livello di servizio erogato, il supporto di secondo livello procede con la chiusura dell'incidente e con la documentazione delle modalità di risoluzione. È avvertito anche il Dirigente dei sistemi informativi che procede con le comunicazioni alla Direzione Generale e il DPO per i casi più gravi o impattanti dal punto di vista dei diritti degli interessati.

Art. 37. - 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 di violazione degli elementi di riservatezza, integrità e disponibilità delle informazioni è necessario avvertire il DPO che provvederà ad eseguire la specifica procedura e documentare l'avvenuta violazione nel registro dei Data Breach.

Art. 38. - Sanzioni

1) Le operazioni effettuate in palese non conformità al presente Regolamento, esporranno alle sanzioni amministrative, civili e penali previste dalla normativa vigente.

Art. 39. - 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 delle sessioni formative e di aggiornamento in modalità frontale o e-learning.
4) Il personale neoassunto è tenuto allo studio del presente regolamento prima del rilascio delle credenziali di accesso al sistema informatico dell'organizzazione.
5) Gli utilizzatori esterni devono essere debitamente informati sul presente Regolamento prima di poter accedere ai sistemi o alla rete di comunicazione.

Glossario

VPN	Rete privata virtuale; modalità di collegamento sicuro alla rete dell'organizzazione
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 dell'organizzazione
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:

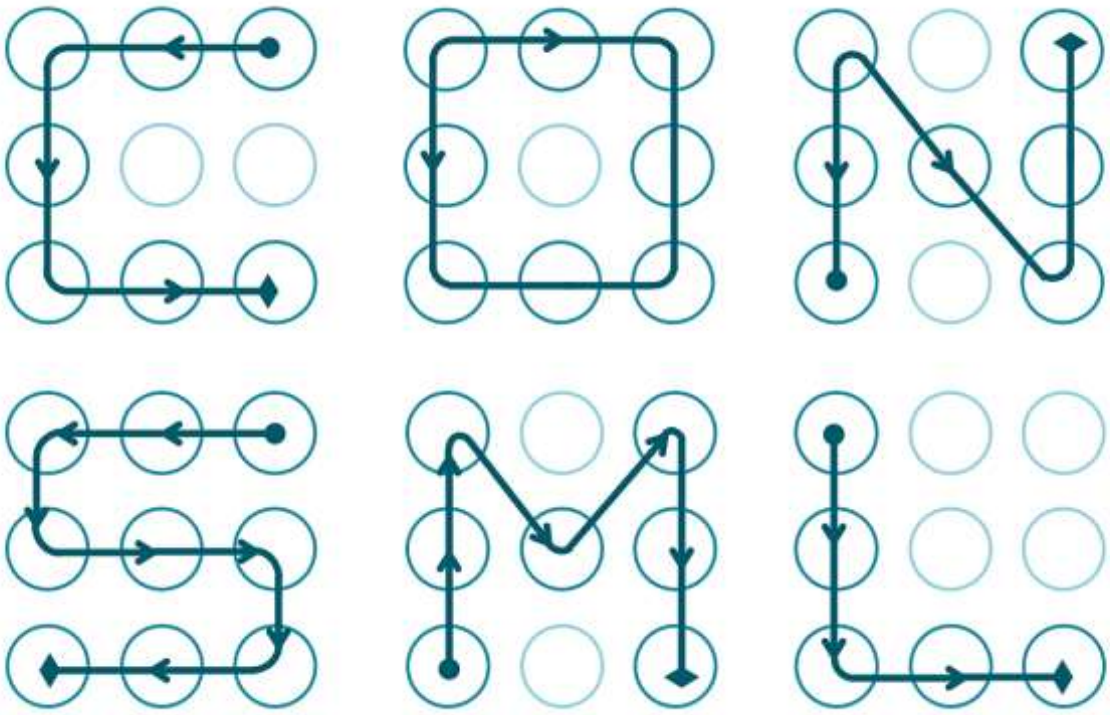
Password	123456	123456789	Qwerty	password
1111111	12345678	abc123	1234567	1234567890
9876543210	password1	12345	letmein	football
iloveyou	admin	welcome	monkey	login
starwars	123123	dragon	passw0rd	master
hello	freedom	whatever	qazwsx	trustno1

In italiano:

123456	123456789	juventus	password	12345678
ciaociao	francesca	alessandro	giuseppe	martina
francesco	valentina	qwertyuiop	antonio	stellina
federico	federica	giovanni	lorenzo	asdasd

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:

Potentially Liable	**Adult/Mature Content**	**Adult/Mature Content**
Child Abuse Discrimination Drug Abuse Explicit Violence Extremist Group Hacking Illegal or Unethical Plagiarism Proxy Avoidance	Advocacy Organizations Alternative Beliefs Dating Gambling Lingerie and Swimsuit Marijuana	Nudity and Risque Other Adult Materials Pornography Sex Education Sports Hunting and War Games Weapons (sales)
Bandwidth Consuming	**Security Risk**	**General Interest – Personal**
Internet Radio and TV Internet Telephony Peer-to-peer File Sharing	Malicious Websites Phishing Spam Urls	Digital Postcards Folklore Games Instant Messaging Social Networking Web Chat

Tali tipologie di siti web sono da considerarsi non correlate alla prestazione lavorativa.

Appendice 4 – Politica sulla criptazione

Data Encryption policy	
Scopo	Il presente documento fornisce le informazioni necessarie per pianificare, preparare e distribuire in modo efficace ed efficiente soluzioni di crittografia al fine di proteggere le informazioni con limitazioni definite a livello legale o contrattuale come ad esempio dati sensibili, per definizione, o dati con valore strategico o rilevanza per l'organizzazione. L'obiettivo della presente politica è definire e fornire una serie di strumenti implementabili nei vari ambiti per l'archiviazione, trasmissione ed elaborazione sicura dei dati "sensibili" per l'organizzazione. Se correttamente implementate, le tecniche crittografiche forniscono un livello elevato di sicurezza tale da evitare accessi non autorizzati alle informazioni nei casi di furto, smarrimento o intercettazione.
Destinatari (Audience)	Tutto il personale interno e gli appaltatori, fornitori e qualsiasi altro soggetto (incluse terze parti) a cui è stato affidato un servizio.
Politica	Tutti i soggetti coinvolti nei servizi e funzioni dell'organizzazione sono tenuti a utilizzare in via esclusiva strumenti di crittografia approvati dall'organizzazione al fine di preservare la riservatezza e l'integrità e controllare l'accessibilità al patrimonio informativo (o parte di esso), specie nei casi di documenti classificati come "Legalmente / contrattualmente limitati" nei casi di elaborazione, archiviazione o trasmissione.
Procedure	Criptazione del settore di boot del disco del dispositivo / sistema *Scenario*: I sistemi mobili (laptop e tablet) contenenti dati sensibili per l'organizzazione potrebbero essere soggetti a furti o a smarrimento. La crittografia a livello di settore di avvio del disco garantisce l'illeggibilità dei contenuti in assenza di specifica chiave. *Prodotti*: BitLocker
	Criptazione degli allegati delle e-mail *Scenario*: L'invio di allegati ai messaggi e-mail contenenti dati sensibili per l'organizzazione deve essere effettuato esclusivamente attraverso la criptazione dei documenti e lo scambio delle chiavi con comunicazione successiva, preferibilmente attraverso altro canale. *Prodotti*: Zip, 7-zip, Win-rar
	Criptazione dei contenuti dei dispositivi portatili (es. unità flash USB) *Scenario*: I dispositivi esterni contenenti dati sensibili per l'organizzazione devono essere criptati nella loro interezza, preferibilmente in modalità nativa o attraverso specifici strumenti di criptazione del singolo documento. *Prodotti*: Zip, 7-zip, Win-rar, unità USB nativamente criptate distribuite dall'organizzazione
	Criptazione degli allegati delle e-mail *Scenario*: In alcuni casi potrebbe essere necessario procedere con la criptazione di singoli documenti o cartelle, locali o di rete. Nel primo caso è possibile effettuare in autonomia la criptazione con gli strumenti in dotazione; per gli altri casi è possibile richiedere ai sistemi informativi specifica impostazione. *Prodotti*: Zip, 7-zip, Win-rar, share di rete nativamente criptata
	Criptazione del livello di trasporto dei contenuti (Transport-Level Encryption)

<table>
<tr><td></td><td>Scenario:
Nelle comunicazioni con soggetti esterni all’organizzazione è sempre buona norma attivare meccanismi di criptazione dei contenuti veicolati. In particolare, è preferibile attivare canali criptati basati su protocolli “secure” e certificati (es. https, ftps, ssh e in generale meccanismi di collegamento IPsec o VPN).
Prodotti:
Client VPN, https tramite certificato o altri protocolli “secure”</td></tr>
<tr><td>Moduli / Istruzioni</td><td>Classificazione dei dati
La classificazione dei dati è il processo nel quale è assegnato uno specifico livello di sensibilità ad un insieme di informazioni trattate, in funzione del grado di controllo e protezione previsti dall’organizzazione. La crittografia deve essere utilizzata per le informazioni considerate sensibili per l’organizzazione, la cui diffusione o semplice condivisione potrebbero arrecare danni anche soltanto reputazionali o di immagine.

Il processo di classificazione dei dati dovrebbe iniziare dal produttore o dall’owner delle informazioni poiché in grado di identificarne con la dovuta precisione valore e potenziale impatto sull’organizzazione.

La classificazione prevede le seguenti denominazioni:
<table>
<tr><td>Strettamente riservate</td><td>Accesso concesso ad un gruppo limitatissimo di soggetti, rigorosamente disciplinati dal principio del “need to know”; sono previsti controlli di sicurezza più stringenti. È prevista la conservazione, preferibilmente in forma criptata ed esclusivamente all’interno del perimetro dell’organizzazione. Non è previsto l’invio tramite posta elettronica, il salvataggio su supporti esterni o la condivisione in cloud.</td></tr>
<tr><td>Riservate</td><td>Accesso concesso ad un gruppo ristretto di utenti in applicazione del principio del “need to know”.
Invio tramite posta elettronica o conservazione al di fuori del perimetro in forma criptata.</td></tr>
<tr><td>Confidenziali</td><td>Accesso concesso a gruppi di utenti dell’organizzazione secondo necessità.
Invio tramite posta elettronica o conservazione al di fuori del perimetro anche in forma non criptata.</td></tr>
<tr><td>Pubbliche</td><td>Accesso senza limitazioni.</td></tr>
</table>
Da notare come alcune tipologie di documenti, pur essendo destinati a divenire pubblici, hanno per obblighi normativi, nel periodo subito precedente alla pubblicazione, un livello di riservatezza comunque elevato. Alcuni documenti di supporto potrebbero dover rimanere comunque riservati o confidenziali</td></tr>
<tr><td></td><td>Selezione e implementazione del prodotto
Sono disponibili sul mercato diverse soluzioni di crittografia. Al fine di garantire un adeguato livello di sicurezza del patrimonio informativo è necessario utilizzare almeno versioni di crittografia allineate almeno ad AES-256 (Word 2016 in poi utilizza questo standard).
Le versioni precedenti dello standard o altri formati potrebbero non essere adeguati alla gestione di contenuti specifici.</td></tr>
<tr><td></td><td>Gestione delle chiavi
Dato che la perdita della chiave di crittografia corrisponde alla perdita dei contenuti del dispositivo o del file/cartella crittografata è fondamentale porre la dovuta</td></tr>
</table>

	attenzione sia alla definizione delle chiavi (in modo da garantire un livello di segretezza granulare) come anche alla conservazione delle stesse. Il personale deputato alla gestione dei file crittografati deve garantire che tutte le chiavi utilizzate nell'archiviazione siano protette e gestite correttamente al fine di garantire il dovuto livello di riservatezza, unitamente all'integrità e disponibilità. Se possibile secondo classificazione, dovrebbe valere la regola di mantenere comunque una copia del documento in forma non criptata nel caso di conservazione all'interno del perimetro aziendale. Le chiavi dovrebbero essere gestite in forma sicura e secondo un ciclo di vita che includa non soltanto la generazione ma più in generale l'uso, l'archiviazione e la distruzione sicura delle chiavi. Deve essere inoltre prevista la procedura nel caso una chiave sia inavvertitamente divulgata o peggio non sia più disponibile. L'accesso alle chiavi di crittografia deve essere permesso alle sole persone di comprovata affidabilità e fedeltà, attraverso specifici accessi con PIN o password, in possesso di almeno due soggetti di livello superiore.
	Cambiamento delle chiavi Nel caso di compromissione delle chiavi è necessario procedere con la modifica controllata e sicura delle chiavi e conseguentemente di tutti i documenti criptati; in questo malaugurato caso è necessario procedere con la revoca, modifica e ridistribuzione di tutte le chiavi interessate. L'operazione, oltre che pericolosa, comporta uno sforzo importante per tutti gli operatori. Riferimenti ISO 27002: 10.8.4, 10.9.1, 10.9.2, 12.2, 12.3

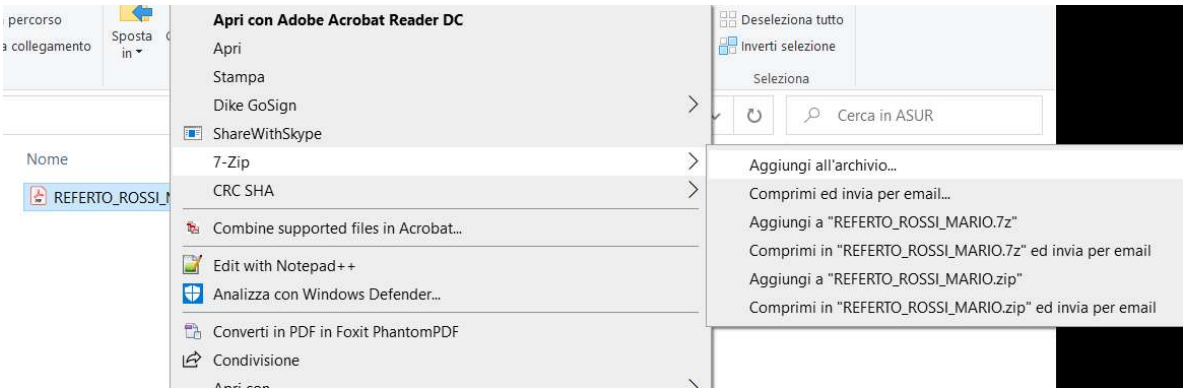
Appendice 5 – Istruzioni per la criptazione dei file tramite 7-zip

Passo 1: scaricate il pacchetto 7-Zip open source da https://www.7-zip.org/download.html dove sono disponibili i pacchetti per i più diffusi sistemi operativi oppure verificare se già installato sul sistema in uso (nel qual caso è possibile saltare il successivo Passo 2).

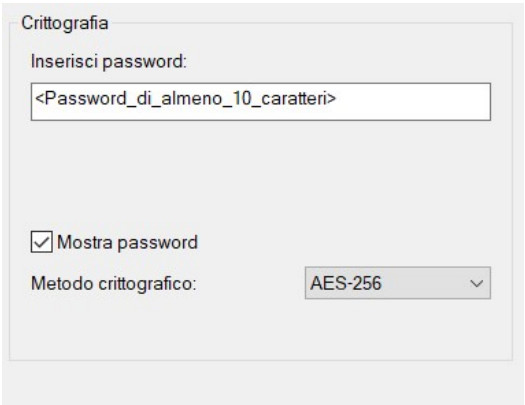
Passo 2: installate 7-Zip; in questo modo, saranno automaticamente integrate le funzioni disponibili nel menu contestuale di Windows Explorer.

Passo 3: selezionate la cartella o il singolo file che desiderate crittografare e fate click con il **tasto destro del mouse**

Passo 4: selezionate "7-Zip" dal menu contestuale e fate clic su "Aggiungi a un archivio..." dal menu pop-up.



Passo 5: inserire la password concordata precedentemente oppure una nuova, da inviare separatamente in una seconda e-mail; la lunghezza deve essere di almeno 10 caratteri e il **Metodo crittografico** di tipo **AES-256**; in questo modo sarà praticamente impossibile ottenere il file senza possedere la chiave.



Passo 6: allegare il file alla e-mail, evitando di riportare nel testo della e-mail ulteriori informazioni

Passo 7: inviare la chiave di decriptazione riportandola nel testo di una seconda e-mail con oggetto identico alla e-mail precedente contenente l'allegato criptato.