Automobile Club d'Italia

Politiche di Sicurezza dei Sistemi e delle Informazioni

2024

A cura della Direzione Centrale Sistemi Informativi e Innovazione

Premessa

Il panorama della sicurezza informatica è in continua evoluzione, e per tale ragione l'adozione di nuovi paradigmi è diventata cruciale al fine di proteggere le risorse delle organizzazioni.

In particolare, negli ultimi anni sono emersi diversi approcci, tra cui spicca il paradigma Zero Trust, rivelatosi essenziale per la difesa contro le minacce cibernetiche che sono sempre più evolute.

Oltre a ciò, il propagarsi del lavoro da remoto e la condivisione sempre più diffusa delle risorse hanno reso obsoleta l'idea tradizionale di un perimetro di sicurezza statico. In questo contesto, il paradigma Zero Trust propone una rivoluzionaria filosofia di sicurezza, basata sull'assunto fondamentale per cui nessuna risorsa o entità all'interno o all'esterno dell'ambiente aziendale dovrebbe essere considerata implicitamente attendibile. Dunque, ogni accesso o transazione deve essere rigorosamente autenticato e autorizzato.

In quest'ottica, l'Ente ha dato avvio al processo di adozione dell'approccio Zero Trust, basato su una strategia di protezione dei sistemi informatici secondo cui nessuna entità (utente, applicativo, servizio o dispositivo) deve essere considerata attendibile automaticamente e il principio dell'accesso alle risorse informatiche è basato su privilegi minimi e attendibilità costantemente rivalutata.

Per nel contesto del nuovo approccio, va in ogni caso riaffermato il principio secondo cui le misure di prevenzione e mitigazione del rischio volte a innalzare la resilienza delle infrastrutture digitali non includono soltanto reti, sistemi e dati ma anche, e soprattutto, utenti la cui consapevolezza – siano essi attori istituzionali, imprese private o cittadini – va alimentata attraverso una diffusa cultura della cybersicurezza. Se ad oggi, infatti, esiste una diffusa percezione dei rischi correlati alla sicurezza fisica, per cui ogni individuo pone in essere, nella propria quotidianità, azioni volte a tutelare sé stesso e i propri beni, lo stesso non può dirsi per la dimensione digitale, dei cui rischi non si ha ancora piena consapevolezza. Tale aspetto, unito alla sempre più ampia disponibilità – a costi relativamente bassi – di strumenti offensivi, all'accresciuto livello di complessità degli attacchi, alla difficoltà tecnica di attribuire gli stessi a un autore certo, nonché alla possibilità che esistano vulnerabilità di sicurezza gravanti su prodotti e soluzioni informatiche, fa registrare un numero complessivo di azioni ostili in costante aumento.

È in questo contesto che si colloca l'esigenza di tutelare i dati e le risorse informatiche dell'Ente, i quali costituiscono un patrimonio sia dal punto di vista informativo che tecnologico. Questo rilevante patrimonio richiede misure di protezione che mirino alla sua salvaguardia. Bisogna allora tutelarne l'integrità e preservarne perdite e manomissioni attraverso il rispetto delle regole a cui deve attenersi chi ha l'accesso alle risorse informatiche e alle informazioni trattate. A questo scopo sono rivolte le regole descritte nel presente documento. Esse costituiscono il riferimento per la definizione delle procedure organizzative da adottare presso le Unità Centrali e Territoriali dell'Ente.

Con il termine "Unità Territoriali" sono indicate per semplicità nel presente documento le Unità Territoriali propriamente dette, le Direzioni Territoriali, le Aree Metropolitane e le Direzioni Compartimentali, se non espressamente definite diversamente. Tali procedure

devono assicurare il corretto svolgimento delle operazioni, attuate dalle diverse figure coinvolte nei processi lavorativi, che utilizzino strumenti informatici. Sono inoltre tracciati i compiti e i ruoli, in materia di sicurezza informatica, di tali figure.

Principio base è che l'accesso alle risorse informatiche (hardware, software, apparati e infrastrutture di rete) e ai dati (documenti cartacei e digitali) può avvenire solo previo rilascio di specifiche autorizzazioni e/o mediante credenziali di autenticazione che permettano il riconoscimento degli utenti.

L'obiettivo del presente documento è quello di fornire le regole di sicurezza in relazione agli aspetti organizzativi, alle modalità di accesso, nonché di gestione dei sistemi informativi presso le Unità Centrali e Territoriali dell'Ente, in linea con la vigente normativa in materia.

Verifiche puntuali e periodiche permetteranno gli indispensabili aggiustamenti, modifiche e/o miglioramenti che dovessero essere ritenuti necessari in seguito a sopraggiunte esigenze dettate da innovazioni tecnologiche e/o evoluzioni normative (attività di audit).

Le novità di questa versione

Sono diverse le novità contenute in questa nuova versione delle Politiche di sicurezza. Tra le più rilevanti è opportuno segnalare l'adeguamento della politica relativa al Responsabile operativo, vale a dire la persona fisica appartenente ad organizzazioni esterne all'Automobile Club d'Italia , dotato di una utenza privilegiata che gli consente di gestire, per conto di quest'ultimo, le utenze relative al personale che presta lavoro all'interno della propria organizzazione inerenti le autorizzazioni, i privilegi ed i diritti di accesso ai dati ed ai servizi.

La politica per il Responsabile operativo è stata adeguata a quanto previsto nel recente Disciplinare a firma del Segretario Generale (prot. 793 del 27/12/2023).

Le Politiche di sicurezza sono inoltre stata adeguate all ultima versione del Codice di Comportamento di Ente (Delibera Consiglio Generale del 24 gennaio 2024), in applicazione della riforma del codice di comportamento dei dipendenti pubblici contenuta nel decreto del Presidente della Repubblica 13 giugno 2°23, n. 81, che modifica il dpr 62/2013.

Sono stati specificati gli adempimenti a cui i Dipendenti devono attenersi in caso di smarrimento del token per la generazione dell'OTP di accesso ad Horizon.

È stato specificato che, in alternativa allo smaltimento, i computer (qualora siano in condizione di potere essere riutilizzati) possono essere donati ad Enti e Organizzazioni no profit e che in tal caso il Dirigente o il Responsabile della Struttura che cura la donazione deve assicurare che l'hard disk sia stato formattato allo scopo di eliminare il rischio della fuoriuscita di dati personali precedentemente memorizzati.

È stato altresì precisato che dalla data della cessazione del servizio, la casella di posta elettronica ordinaria viene resa non più accessibile. Il dipendente (prima della data di cessazione) può inserire un messaggio automatico che avvisi che la casella non è più presidiata e che inviti a scrivere (per le comunicazioni di servizio) ad una diversa casella

individuata in accordo con il Responsabile della Struttura di appartenenza, ed eventualmente anche ad una casella personale (non di servizio) per le eventuali comunicazioni di carattere personale.

Tutte le altre utenze devono essere disattivate entro dieci giorni.

È stato specificato che qualora per esigenze di servizio si abbia comunque la necessità di accedere ad un sito da Horizon (il quale, per esigenze di sicurezza, ha dei vincoli più stringenti rispetto alla navigazione fuori Horizon), il Direttore o il Responsabile della Struttura potrà fare richiesta motivata di sbloccare l'accesso ad uno specifico sito.

La gestione degli incidenti (cap. 9) è stata interamente rivista, anche alla luce di una apposita sperimentazione che è stata effettuata allo scopo di testare le procedure organizzative che è necessario attivare nel momento in cui si verifica un evento potenzialmente rischioso per la sicurezza. La gestione è stata in particolare semplificata, riducendo il numero di passaggi, allo scopo di ridurre i tempi di reazione e circoscrivere nel più breve tempo possibile i potenziali danni.

È stato esplicitato il divieto di utilizzare gli account istituzionali per la registrazione su siti esterni per motivi personali, salvo essendone consentito l'utilizzo solo se necessario per esigenze di servizio. La registrazione su siti esterni rende peraltro più facilmente intercettabili le credenziali, e pertanto è un potenziale fattore di rischio per la sicurezza.

È stato precisato che la richiesta di installazione su postazioni di singoli Dipendenti di programmi software non compresi nella dotazione standard deve essere preventivamente approvata dal Direttore delle Struttura di appartenenza e autorizzata dalla Direzione Sistemi Informativi e Innovazione.

È stato precisato che il primo invio delle credenziali può essere effettuato verso un indirizzo mail personale. In tal caso la procedura deve tuttavia prevedere il cambio password automatico al primo accesso.

È stata inserita la raccomandazione di non utilizzare pen-drive per il trasferimento dei dati ed è stato precisato che la modalità normale per trasferire documenti e file è costituita dalla posta elettronica e Drive.

Acronimi e Definizioni

Accesso logico	L'utilizzo di una particolare risorsa informatica da parte dei soggetti richiedenti
Assegnatario	Dipendente ACI o collaboratore esterno cui viene assegnata una determinata dotazione informatica e che pertanto è responsabile per la sua custodia e corretto utilizzo. Non necessariamente coincide con l'utilizzatore finale della dotazione.
Asset Management	Insieme di processi, best practice, strumenti, risorse e competenze finalizzate alla gestione strutturata e sistematica dell'intero ciclo di vita degli asset.
Autenticazione	L'attività svolta da un apposito "sistema di controllo degli accessi logici" per assicurarsi dell'autenticità dell'identità del soggetto richiedente (tipicamente tramite l'uso di password).
Autorizzazione	L'attività di verifica svolta da un apposito "sistema di controllo degli accessi logici" della corrispondenza tra i privilegi esistenti in capo al soggetto richiedente, identificato nei sistemi informativi, e il tipo di operazione che il soggetto è abilitato ad eseguire.
BC	Business Continuity, capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente.
Cartella condivisa	Area di memorizzazione per informazioni in formato elettronico accessibile a più utenti, sia locale (su postazione di lavoro), sia remota (su server di rete).
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.
Credenziali	L'insieme degli elementi identificativi di un utente o di un account; nella pratica comune si utilizza spesso, come credenziale di accesso, la coppia formata da un codice identificativo (User ID) e da una parola chiave segreta (Password) per accedere ad una risorsa o ad un sistema.
Crisi	Evento straordinario scaturito dall'escalation di uno o più incidenti, con la potenzialità di compromettere, in modo permanente o per un periodo prolungato, le funzionalità di uno o più asset strategici per l'attività aziendale, e che può richiedere l'attivazione di soluzioni di Business Continuity e Disaster Recovery.
DR	Disaster Recovery, l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
DSII	Direzione Sistemi Informativi e Innovazione
Evento di sicurezza	Occorrenza dello stato di un sistema, servizio o rete che indichi una potenziale infrazione di una politica di sicurezza o il fallimento di un controllo, o il verificarsi di una situazione precedentemente ignota e potenzialmente rilevante per la sicurezza delle informazioni.

Fake news	Contenuto informativo falso o distorto, artatamente costruito, il cui deliberato utilizzo è volto ad ottenere un vantaggio politico o finanziario illecito.
Falso positivo	Evento che si rivela, in seguito ad analisi, non rilevante in termini di sicurezza.
ICT	Information & Communication Technology.
Identificazione	L'attività svolta da un apposito "sistema di controllo degli accessi logici" per riconoscere l'identità del soggetto richiedente (tipicamente tramite la verifica dell'esistenza della utenza presentata).
IDS	Intrusion Detection System, dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali.
Incidente di sicurezza	Evento o sequenza di eventi di sicurezza indesiderati che comportano una significativa probabilità di compromissione delle operazioni di business e della sicurezza delle informazioni, intesa come integrità, disponibilità e riservatezza del patrimonio informativo.
Intelligenza Artificiale (IA)	Disciplina che si occupa dello studio di funzioni tipiche dell'intelligenza umana e della loro possibile replicazione mediante metodi e strumenti informatici.
IPS	Intrusion Prevention System, componenti software attivi sviluppati per incrementare la sicurezza informatica di un sistema informatico, individuando, registrando le informazioni relative e tentando di segnalare e bloccare le attività dannose.
Lesson Learnt	Informazioni utili alla gestione degli incidenti di sicurezza ricavate dalla gestione di eventi ed incidenti pregressi.
Log	Un log è il risultato di una registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico, sia esso un server, un client, un'applicazione o un programma.
Mailing-list	Lista di distribuzione automatica di messaggi di posta elettronica, riguardanti un determinato argomento. I messaggi sono inviati ad un list server che provvede ad inviarli automaticamente agli iscritti.
Peer to Peer (P2P)	Meccanismo di condivisione di contenuti digitali tramite una rete di computer paritetici, più frequentemente utilizzati per scambio di file con contenuti audio, video, dati e software.
Posta Elettronica Certificata (PEC)	Servizio per la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna, secondo quanto previsto in materia di trasmissione di dati e documenti informatici dal D.P.R. n. 68/2005.
Privilegio	La delega di autorità su una determinata risorsa informatica. Il privilegio permette agli utenti di eseguire azioni su una determinata risorsa, come ad esempio l'accesso a un servizio o la lettura e la scrittura di un file.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i

	trattamenti ad essa consentiti.
Referenti dei dati e delle applicazioni	Direzioni e Uffici Centrali responsabili delle banche dati di rispettiva competenza (vedi paragrafo Classificazione delle informazioni).
Responsabile operativo	Figura appartenente a unità organizzativa esterna, cui ACI concede privilegi di gestione locale delle utenze.
RID	Riservatezza - Integrità - Disponibilità.
Rischio di sicurezza	Rischio di perdita dei requisiti di riservatezza, integrità e disponibilità delle informazioni.
Root Cause Analysis	Tecnica di indagine sistematica che viene applicata ad eventi di particolare impatto, in particolare incidenti, ed è finalizzata ad esaminare quanto accaduto ricercandone le cause.
SEM	Security event management, soluzione software che, in tempo reale, provvede al monitoraggio e alla gestione degli eventi che accadono all'interno della rete e sui vari sistemi di sicurezza, fornendo una correlazione e aggregazione tra essi. L'interfaccia è una console centralizzata, preposta ad attività di monitoraggio, segnalazione e risposta automatica a determinati eventi.
SIEM	Security Information & Event Management, serie di prodotti software e servizi che combinano/integrano le funzionalità offerte dai SIM a quelle dei SEM
SIM	Security Information Management, sistema di gestione delle informazioni che automatizza il processo di raccolta e orchestrazione dei log (ma non in tempo reale). I dati vengono raccolti e spediti ad un server centralizzato tramite l'utilizzo di software agent installati sui vari dispositivi del sistema monitorato. La possibilità di usufruire di spazi di archiviazione a lungo termine unita all'analisi dei dati consente la generazione di report personalizzati.
Sistema informativo	Insieme discreto e delimitato di risorse informative progettato, costruito, gestito e mantenuto per raccogliere, registrare, elaborare, archiviare, recuperare, visualizzare e trasmettere determinate informazioni.
Spam	Invio di grandi quantità di messaggi indesiderati (generalmente commerciali) che può essere attuato attraverso vari mezzi di comunicazione, in particolare tramite la posta elettronica.
SW	Software
Utenti	Le persone fisiche che fanno uso di sistemi di elaborazione dei dati, a ciascuno dei quali, identificato personalmente, è associata una o più utenze.
Utenza o User ID	Entità logica che permette di identificare un utente all'interno di una risorsa informatica
VPN	Una Virtual Private Network è una rete privata virtuale instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso

come internet. Lo scopo delle reti VPN è di garantire un livello di sicurezza pari o superiore ad una connessione dedicata, utilizzando reti pubbliche condivise.

Workaround Metodo temporaneo per raggiungere una soluzione.

1. Politiche di Sicurezza delle Informazioni

L'Automobile Club d'Italia opera in un contesto molto vasto e complesso, le informazioni aziendali sono, ormai, quasi interamente gestite in forma elettronica ed i sistemi informatici sono utilizzati da un numero crescente di persone, interne ed esterne, con una variabilità elevata di utenti e di collegamenti. Questa realtà, se da un lato assicura la disponibilità di informazioni sempre aggiornate, dall'altro enfatizza il sorgere di rischi connessi alla loro protezione e controllo, che richiedono la presenza di misure idonee a rendere sicuro il patrimonio informativo.

L'Automobile Club d'Italia, ritenendo prioritario assicurare la sicurezza delle informazioni, declinata come sicurezza informatica dei sistemi e dei processi organizzativi connessi, ha investito su di essa come progetto strategico e ha deciso di adottare una serie di requisiti volti a proteggere le risorse informatiche aziendali, ivi comprese le informazioni trattate.

L'ACI evidenzia una serie di requisiti che rappresentano il punto di riferimento principale cui tutti devono tendere nel loro operare quotidiano; nel caso in cui si presentino situazioni nelle quali questi requisiti non possano trovare completa attuazione dovrà essere predisposta un'idonea valutazione dei rischi e formulato un piano di lavoro per il pronto ripristino delle condizioni di sicurezza. I requisiti e le responsabilità esplicitati nei successivi paragrafi sono pienamente aderenti a:

- Direttiva della Presidenza del Consiglio dei Ministri del 16/01/02 sui requisiti minimi di sicurezza.
- Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione del marzo 2004 a cura del Comitato tecnico nazionale sulla sicurezza informatica e delle Telecomunicazioni nelle Pubbliche amministrazioni.
- La sicurezza dei servizi in rete — requisiti, modelli, metodi e strumenti a cura AIPA del 14/11/01.
- Linee guida in tema di sicurezza informatica a cura AIPA del 2/10/99.
- Circolare AGID 18 aprile 2017, n. 2 "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)"
- Regolamento (UE) 2016/679 – General Data Protection Regulation (GDPR).
- Codice in materia di protezione dei dati personali D.lgs. N° 196/2003, come modificato dal D.Lgs. n. 101/2018.
- DPCM del 17 febbraio 2017, che ha aggiornato l'architettura nazionale di sicurezza cibernetica già delineata dal DPCM del 23 gennaio 2013;
- Decreto legislativo 18 maggio 2018, n. 65, che prevede obblighi sia di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi forniti, sia di implementazione di misure di sicurezza basate sull'analisi del rischio per gli Operatori di Servizi Essenziali e i Fornitori di Servizi Digitali;
- Decreto-legge 21 settembre 2019, n. 105, che ha istituito il Perimetro di sicurezza nazionale cibernetica, con l'obiettivo di tutelare gli asset digitalizzati dal cui malfunzionamento, interruzioni, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, prevedendo, rispetto al decreto NIS, più stringenti criteri di notifica degli incidenti e maggiori livelli di sicurezza, estesi

anche alla supply chain, nonché specifiche procedure in materia di procurement ICT ad essi destinati;

- Decreto-legge 19 luglio 2020, n. 76, che ha fornito impulso alla digitalizzazione della PA, prevedendo che la stessa avvenga osservando principi di sicurezza cibernetica compresa la formazione del personale e la promozione della consapevolezza circa l'importanza della sicurezza informatica;
- Decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;
- Strategia Cloud Italia, adottata nell'ambito del Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022 e definita dal Dipartimento per la trasformazione digitale in collaborazione con l'Agenzia per la Cyber- sicurezza Nazionale, al fine di incentivare la diffusione di soluzioni basate sul cloud computing nel circuito delle Pubbliche Amministrazioni;
- Decreto legislativo 8 novembre 2021, n. 207, di Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche e disciplina, tra l'altro, i requisiti di cybersicurezza delle reti pubbliche di comunicazione o dei servizi di comunicazione elettronica accessibili al pubblico, l'obbligo di notifica di incidenti significativi, nonché l'adozione di misure di sicurezza, attribuendo la competenza in materia all'ACN;
- Decreto-legge 21 marzo 2022, n. 21, che ha recato, tra le varie, disposizioni sulla ridefinizione dei poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché di ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud. In particolare, ha ridefinito gli obblighi e le procedure di notifica da parte delle imprese interessate, nonché le procedure di esercizio dei poteri speciali, di monitoraggio e sanzionatori da parte del Governo, preve- dendo la partecipazione dell'Agenzia per la Cybersicurezza Nazionale, la possibilità di avvalersi anche del Centro di Valutazione e Certificazione Nazionale (CVCN) e la possibilità di condurre attività ispettive e di verifica;
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)
- Strategia Nazionale di Cybersicurezza 2022 – 2026 dell'Agenzia per la Cybersicurezza Nazionale e Piano di implementazione delle misure;
- Ordinamento dei servizi dell'Automobile Club d'Italia;
- Codice di Comportamento di Ente (Delibera Consiglio Generale del 20 febbraio 2014) (Delibera Consiglio Generale del 22 luglio 2015, Delibera Consiglio Generale del 8 aprile 2021, Delibera Consiglio Generale del 24 gennaio 2024);
- Convenzione tra ACI e la Società ACI Informatica SpA.

1.1. Responsabilità

Il Direttore della Direzione Sistemi Informativi e Innovazione è responsabile della promozione e diffusione delle misure organizzative e normative di sicurezza informatica (procedure e standard) e ha l'incarico di mettere a disposizione gli strumenti tecnici più idonei per la riduzione dei rischi in materia.

Come Responsabile della Sicurezza informatica, coadiuvato dall'Ufficio per l'Organizzazione Digitale, assicura i seguenti compiti:

- definire i princìpi generali di utilizzo dei sistemi e degli apparati informatici;
- definire le regole e le procedure di sicurezza informatica cui tutto il personale dovrà ottemperare;
- definire gli obiettivi di sicurezza che ACI Informatica SpA, quale realizzatore e gestore dei sistemi informativi ACI, dovrà attuare nelle attività di progettazione ed esercizio dei sistemi informatici di ACI;
- monitorare i rischi informatici.

Le figure organizzative, sono tenute a operare nello spirito della presente normativa e a promuovere un ambiente protetto e controllato; inoltre, essi devono assicurare il rispetto dei criteri di accessibilità, riservatezza e di protezione dei dati di loro pertinenza.

1.2. Princìpi

La Sicurezza delle Informazioni trova fondamento nei seguenti princìpi.

Le apparecchiature e gli strumenti informatici, installati negli Uffici dell'Ente, devono essere utilizzati esclusivamente per gestire le attività dell'Ente, in linea con le autorizzazioni rilasciate.

Le risorse informatiche devono essere protette da danneggiamenti, furti e cause che possono compromettere il servizio alle attività aziendali; le apparecchiature fanno capo all'assegnatario, individuato secondo la normativa contabile vigente, il quale deve attivare ogni iniziativa utile alla loro protezione.

Le risorse informatiche (dati, programmi, apparecchiature) devono essere classificate con riguardo alla loro importanza, rese disponibili solo alle persone autorizzate e trattate in conformità.

I dati e le informazioni fanno capo al Direttore Centrale della Direzione/Servizio/Ufficio che istituzionalmente li origina e li utilizza per la gestione delle operazioni di competenza. Egli assicura la definizione del loro livello di accessibilità, di riservatezza e delle misure organizzative di controllo idonee a proteggerle.

Il dipendente è responsabile della protezione e conservazione dei dati, compresi i codici di accesso ai programmi e agli strumenti informatici avuti in dotazione per l'espletamento dei

propri compiti, ed è tenuto all'utilizzo di tali strumenti in modo appropriato e conforme ai fini istituzionali.

Il dipendente è responsabile della protezione e conservazione dei dati, compresi i codici di accesso ai programmi e agli strumenti informatici avuti in dotazione per l'espletamento dei propri compiti, ed è tenuto all'utilizzo di tali strumenti in modo appropriato e conforme ai fini istituzionali.

Il dipendente, nel caso in cui rilevi la perdita di dati informatici o la compromissione dell'accesso o la divulgazione indebita è obbligato a darne immediata comunicazione al dirigente o responsabile della Struttura di appartenenza.

Il dipendente, che venga a conoscenza di problematiche o malfunzionamenti riguardanti la propria attività o le funzioni dell'Ente, evita di darne pubblicità e provvede tempestivamente a darne segnalazione all'interno dell'Ente.

I dirigenti e i responsabili di Struttura devono, in ragione del ruolo, degli incarichi e delle funzioni loro assegnate, vigilare in merito all'applicazione delle disposizioni sull'utilizzo delle tecnologie informatiche e dei dispositivi elettronici personali[1].

L'autorizzazione all'uso delle risorse deve essere correlata alle effettive esigenze per l'espletamento delle specifiche attività lavorative, secondo le autorizzazioni rilasciate dalle unità competenti.

Le applicazioni devono essere classificate in funzione del loro livello di sicurezza, in particolare le applicazioni considerate critiche o che comportano il trattamento di dati personali devono essere:

- dotate di strumenti che impediscano accessi non autorizzati e che segnalino tempestivamente la presenza di eventi anomali;
- dotate di strumenti e tecniche che garantiscano l'integrità, la disponibilità e la verificabilità delle operazioni attuate attraverso gli strumenti informatici; deve essere inoltre assicurata l'integrità dei dati, dei programmi e delle elaborazioni, nonché la continuità del servizio informatico (*business continuity*).

La rete di comunicazione deve essere dotata di apparecchiature e di misure di controllo per la protezione da intrusioni o intercettazioni dei dati aziendali; i collegamenti con risorse informatiche non sotto il governo diretto di ACI devono essere gestiti con misure di controllo atte a impedire accessi non autorizzati.

I dati personali, relativi a dipendenti e a terzi, devono essere considerati e trattati in modo riservato ed esclusivamente nell'ambito dell'attività lavorativa di competenza; non è ammessa la creazione di archivi elettronici di dati personali che non sia stata preventivamente autorizzata dal Titolare. I princìpi di sicurezza delle informazioni sopra descritti trovano pratica attuazione nei seguenti "programmi" specifici.

[1] V. art. 16 Codice di comportamento

1.2.1 Protezione fisica delle risorse

La protezione fisica delle risorse si attua mediante:

- la classificazione delle aree aziendali secondo la loro criticità operativa;
- l'accesso controllato alle aree considerate critiche;
- la sicurezza fisica e la sorveglianza di queste aree e dei beni in esse contenuti.

1.2.2 Classificazione delle informazioni

Le informazioni aziendali, in qualsiasi forma siano espresse (posta elettronica, archivi informatici, documenti, ecc.), devono essere protette con regole e misure tecniche correlate alla loro importanza (riservatezza, criticità, ecc.) sia ai fini aziendali che di legge.

Le misure di protezione (informatiche e non) vanno estese anche a soggetti esterni che dispongono delle informazioni a seguito di obblighi contrattuali.

1.2.3 Sicurezza informatica

Fanno parte del programma i seguenti elementi:

- il controllo degli accessi ai dati e alle risorse informatiche, nonché il mantenimento della loro disponibilità e integrità;
- la sicurezza nella trasmissione e nelle comunicazioni all'interno di ACI e con l'esterno;
- la sicurezza delle stazioni di lavoro e dei personal computer;
- la sicurezza nel processo di sviluppo delle applicazioni informatiche;
- la sicurezza nella gestione operativa delle installazioni informatiche;
- la protezione degli output dei sistemi informatici (stampe, nastri, DVD, ecc.) negli uffici operativi.

1.3 La cultura delle sicurezza

Da non trascurare infine, l’importanza della diffusione della cultura della sicurezza tra tutti i componenti della organizzazione. Saper usare un computer o un qualunque dispositivo informatico aumenta la consapevolezza dei rischi a cui si va incontro e delle conseguenze del comportamento non virtuoso.

L’Agenzia per la Cybersicurezza Nazionale ha evidenziato, nell’ambito della Strategia Nazionale di Cybersicurezza 2022 – 2026 come sia indispensabile fare riferimento a una serie di fattori abilitanti – formazione, promozione della cultura della sicurezza cibernetica e cooperazione – i quali, data la loro trasversalità, sono necessariamente correlati a tutti e tre gli obiettivi sopra delineati, quali elementi imprescindibili per la loro piena attuazione.

In particolare, la promozione della cultura della sicurezza cibernetica, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber.

Fa parte della mission della Direzione Sistemi Informativi e Innovazione la formazione del personale in ambito sicurezza. Buona parte degli attacchi hacker, in questo periodo storico, hanno avuto successo proprio grazie a disattenzioni e negligenze da parte dei componenti dell'organizzazione, per questo è fondamentale che ogni dipendente studi e conosca il comportamento migliore atto a mitigare i rischi , sia consapevole e responsabile, inoltre, rispetto agli accorgimenti da interiorizzare come abitudini, rispetto al riconoscimento dei campanelli di allarme, rispetto alle azioni da compiere e a quelle da evitare assolutamente.

L’obiettivo della formazione è pertanto di mostrare il collegamento tra il rischio cyber e l’elemento umano.

2. Standard e regole di Sicurezza delle Informazioni

La presente sezione descrive le regole di Sicurezza delle informazioni adottate in ACI.

Queste regole costituiscono il punto di riferimento per la messa a punto delle misure tecniche e degli strumenti di protezione delle risorse informatiche. La loro realizzazione nei diversi settori di competenza sarà graduale: il Responsabile della Sicurezza promuoverà la loro attivazione secondo priorità ed opportunità che verranno via via decise dal Direttore della Direzione Sistemi Informativi e Innovazione.

Il dipendente è tenuto al rispetto di quanto previsto dalle regole di sicurezza informatica e da ogni altra disposizione sull'utilizzo delle tecnologie informatiche, al fine di non compromettere la funzionalità e la protezione dei sistemi informatici.[2]

Le regole potranno variare nel tempo in relazione ai cambiamenti di tipo tecnologico, organizzativo e strutturale, e ai cambiamenti di tipo legislativo: il Responsabile della Sicurezza procederà al loro aggiornamento.

2.1. Introduzione

Gli standard di Sicurezza delle informazioni costituiscono il punto di riferimento primario per la formulazione delle normative in materia.

Essi rappresentano, nel loro insieme, il modello attuativo delle misure di Sicurezza adottate da ACI ed il quadro entro cui definire i rischi.

In particolare:

- gli standard definiscono una serie di obiettivi di Sicurezza e di regole volte alla realizzazione del modello di Sicurezza definito per l'Ente. Essi si strutturano in aree specialistiche e possono essere corredati da modalità attuative che ne facilitano l'interpretazione;
- le normative rappresentano la traduzione degli standard nel modus operandi. Esse si articolano in procedure che devono essere distribuite alle unità organizzative e al personale, secondo la rispettiva competenza. La normativa può assumere la forma di guida tecnica, qualora lo standard riguardi le misure tecniche da attuare in riferimento a prodotti hardware e software di sicurezza;
- la conduzione delle attività quotidiane da parte degli utenti operativi e degli utenti tecnici è guidata dalle procedure e dalle guide: può accadere che queste regole non vengano sempre puntualmente osservate e che i responsabili e il personale adottino iniziative di compromesso. Queste situazioni determinano l'insorgere di rischi informatici che devono essere adeguatamente monitorati attraverso le procedure di gestione della Sicurezza.

[2] V. art. 16 del Codice di comportamento

Nei paragrafi che seguono, vengono illustrati gli standard e le conseguenti regole distinte per aree specialistiche.

2.2. Classificazione delle informazioni

Il patrimonio informativo gestito dall'ACI è riconducibile ai seguenti ambiti.

Banca dati Pubblico Registro Automobilistico (PRA), il cui trattamento dati è finalizzato alla tenuta, attraverso procedure automatizzate e tecniche elettroniche, del Pubblico Registro Automobilistico secondo le modalità di cui alla legge istitutiva e delle successive integrazioni e modificazioni, nonché per finalità connesse e/o per l'assolvimento dei compiti istituzionali ACI.

Banca dati Tasse, il cui trattamento dati è finalizzato alla riscossione delle tasse automobilistiche e alla tenuta e gestione dell'archivio dei veicoli assoggettati al pagamento; all'effettuazione del riscontro e controllo di merito dei pagamenti effettuati e, infine, allo svolgimento delle attività dirette al recupero, in via bonaria, delle somme dovute dai contribuenti a seguito dei riscontri e controlli effettuati. Con l'art. 51 del Decreto-Legge 26 ottobre 2019, n. 124, al sistema informativo del pubblico registro automobilistico, ai sensi e per gli effetti dell'articolo 5 del decreto-legge 30 dicembre 1982, n. 953, convertito, con modificazioni, dalla legge 28 febbraio 1983, n. 53, sono acquisiti anche i dati delle tasse automobilistiche, per assolvere transitoriamente alla funzione di integrazione e coordinamento dei relativi archivi. I predetti dati sono resi disponibili all'Agenzia delle entrate, alle regioni e alle Province autonome di Trento e di Bolzano, le quali provvedono a far confluire in modo simultaneo e sistematico i dati dei propri archivi delle tasse automobilistiche nel citato sistema informativo.

Banca dati Soci dell'Automobile Club d'Italia, il cui trattamento dati è finalizzato alla gestione della base associativa in termini amministrativi e di erogazione dei servizi previsti.

Banca dati del personale dipendente di ACI, il cui trattamento dati è inerente alla elaborazione del trattamento giuridico ed economico del personale, alla selezione, alla rilevazione delle presenze, alla formazione del personale.

Banca dati dei servizi amministrativi, il cui trattamento dati è inerente alla gestione amministrativa della clientela e dei fornitori.

Banca dati Licenziati sportivi, il cui trattamento è finalizzato alla gestione dei dati personali relativi ai titolari di licenza sportiva.

Banca dati sito internet ACI, il cui trattamento investe l'insieme dei dati personali acquisiti con la registrazione degli utenti.

Ogni ulteriore banca dati che dovesse costituirsi nel rispetto della Convenzione vigente tra ACI e ACI Informatica SpA.

Per quanto riguarda le categorie di dati particolari e i dati personali relativi a condanne penali e reati, di cui agli artt. 9 e 10 del Regolamento UE 679/2016 (GDPR), si indicano i dati

oggetto di trattamento da parte del Sistema Informativo per i quali si devono adottare specifiche cautele:

- dati relativi all'iscrizione ai sindacati da parte del personale ACI;
- dati relativi a trattenute sullo stipendio dovute a motivi di salute o a provvedimenti giudiziari;
- dati riguardanti le assenze per motivi di salute del personale ACI;
- dati riguardanti l'esenzione per i disabili in materia di tasse automobilistiche e PRA;
- dati riguardanti le riduzioni di tariffa della tessera di socio ACI per gli appartenenti a particolari categorie.

L'applicazione delle misure riguardanti le tipologie di dati sopraindicate deve riferirsi anche alle fattispecie in cui l'informazione da proteggere possa desumersi indirettamente.

2.3. Standard di sicurezza informatica

2.3.1. Area: protezione delle risorse. Assegnazione di risorse informatiche

Obiettivo: *definire per ogni risorsa informatica una precisa responsabilità*

Regole:

1. Ogni applicazione informatica e ogni data set di informatica aziendale e/o individuale devono essere assegnati ad un Direttore Centrale/Dirigente/Responsabile, secondo competenza.
2. Ogni risorsa informatica, centrale o periferica (hardware) e i relativi sistemi e sottosistemi operativi (SW di base), devono essere assegnati ad una Unità Organizzativa (Direzione/Servizio Centrale, Ufficio Centrale/Periferico) che, a sua volta, ne destinerà l'uso al dipendente.
3. Le responsabilità da assegnare sono:

   a. *Sistemi centrali e di rete:* la Direzione Sistemi Informativi e Innovazione acquisisce, gestisce e custodisce le risorse; per convenzione ACI può delegare tali attività, in tutto o in parte, alla propria soc. ACI Informatica SpA.

   b. *Installazioni periferiche*: la Direzione Sistemi Informativi e Innovazione acquisisce le risorse hardware secondo la normativa vigente; per convenzione ACI può delegare tale attività, in tutto o in parte, alla propria soc. ACI Informatica SpA; la custodia delle stesse è assegnata al Responsabile dell'Unità Organizzativa ricevente (es.: il Responsabile dell'Unità Territoriale).

   c. *Procedure applicative e dati*: la gestione e la custodia sono assegnate alle Unità Organizzative a eccezione di applicazioni e dati di natura web la cui conservazione avviene su server aziendali protetti della soc. ACI Informatica SpA.

4. L'assegnazione delle responsabilità, inerenti l'hardware ed il software di base, deve avvenire al momento della loro installazione; per il software applicativo,

l'individuazione dell'assegnatario deve avvenire nel momento in cui si decide di rilasciare una nuova applicazione.
5. L'assegnazione della proprietà delle risorse e delle applicazioni deve essere formalizzata e resa disponibile alla Direzione Sistemi Informativi e Innovazione e aggiornata in relazione ai cambiamenti organizzativi.

2.3.2. Area: protezione delle risorse. Accessi fisici alle installazioni

Obiettivo: *proteggere le aree aziendali in relazione alle attività che in esse vengono espletate e permettere l'accesso solo alle persone autorizzate.*

Regole:

1. Le aree aziendali devono essere classificate e protette in relazione al valore delle informazioni che sono trattate o sono ivi disponibili.
2. I locali dell'Ente in cui sono installati apparati informatici possono essere classificati aree riservate ad accesso controllato: l'accesso è autorizzato dal Direttore della Direzione Sistemi Informativi e Innovazione o persona da questi delegata e deve essere consentito esclusivamente per esigenze di lavoro. Sono aree riservate anche i locali in cui sono installati apparati di comunicazione e i server di rete: l'accesso è gestito dal responsabile della loro custodia.
3. Le misure di controllo degli accessi possono prevedere il ricorso a dispositivi e tecniche di controllo che permettano l'accesso solo alle persone autorizzate e che ne registrino i movimenti.
4. Il personale interno, non addetto alle aree riservate, può accedervi esclusivamente per motivi di lavoro e solo previa autorizzazione.
5. Il personale esterno deve essere identificato al momento dell'ingresso; durante la permanenza nei locali dell'Ente, deve essere sempre accompagnato da uno specifico dipendente, ad eccezione degli Organi di Polizia Giudiziaria, per gli specifici compiti loro assegnati in materia di indagini, ispezioni, ecc..
6. Il personale addetto ai servizi (pulizia, manutenzioni, ecc.) deve essere identificato sulla base di comunicazioni (liste di riconoscimento) specifiche.

2.3.3. Area: protezione delle risorse. Protezione delle stazioni di lavoro

Obiettivo: *proteggere e controllare l'utilizzo degli strumenti hardware e software installati e garantire l'integrità dei dati, oltre che l'uso esclusivo ai fini aziendali.*

Regole:

1. È responsabilità dell'utente mettere in atto tutte le precauzioni necessarie al fine di evitare l'accesso alla risorsa da parte di soggetti non autorizzati ogni qualvolta ci si allontana dall'apparecchiatura (ad es. procedere al blocco del computer; attivazione dello screensaver protetto da password; ecc.).

2. È responsabilità dell'utente evitare di lasciare le pratiche sulla scrivania, sui tavoli di lavoro o comunque a portata di mano, se non per il tempo necessario all'effettivo utilizzo. Al termine della giornata tale documentazione deve essere riposta all'interno degli archivi.
3. Nella lavorazione in smart working l'utente deve avere cura di proteggere le informazioni accessibili dalla postazione utilizzata da eventuali terzi presenti nel medesimo ambiente.
4. È responsabilità dell'utente usare la stazione di lavoro in modo protetto ed esclusivamente per motivi di lavoro: le credenziali di accesso devono essere tenute riservate.
5. Su disco fisso non devono essere memorizzate informazioni classificate riservate o segrete se non adeguatamente protette (ad esempio attraverso la crittografia). Il disco fisso, se contiene dati riservati o segreti, deve essere formattato prima che il personal computer (o server) venga assegnato ad altra unità organizzativa; nel caso che l'apparecchiatura richieda interventi tecnici (es.: manutenzione), devono essere adottate norme comportamentali che impediscano, salvo cause di forza maggiore, che la stessa venga portata all'esterno.
6. È fortemente consigliato conservare file e dati su Drive, e mantenerli memorizzati su disco fisso solo nei casi in cui per ragioni di servizio sia indispensabile.
7. Qualora per esigenze di servizio sia necessario conservare i dati sul proprio computer e/o su cartelle condivise, anziché su Drive, i dati contenuti nel disco fisso devono essere sottoposti a salvataggio da parte del dipendente con frequenza commisurata alla loro criticità e, comunque, almeno una volta al mese. Di norma, tale operazione viene eseguita tramite ausilio del cloud aziendale o, eccezionalmente, su dispositivi esterni (hard disk; CD; DVD e Blu-Ray; pen/flash drive) di proprietà dell'Ente e autorizzati dal Direttore dei Sistemi Informativi e, in generale, su supporti rimovibili (es.: microSD nel caso di smartphone o tablet).
8. Lo scarico su supporti destinato all'esterno dell'unità organizzativa richiedente, deve essere giustificato e autorizzato dal Direttore Responsabile.
9. Tutti i computer assegnati ai dipendenti hanno un profilo utente vincolato, tranne nei casi autorizzati dal Direttore DSII per specifiche esigenze di servizio.
10. Un pacchetto software in dotazione alle stazioni di lavoro è considerato ufficiale ed autorizzato solo quando fornito dal Sistema Informativo; sono ammesse eccezioni solo per i pacchetti ricevuti da Enti esterni qualificati e riconosciuti.
11. Il pacchetto software in dotazione non deve essere modificato; quando associato ad una stazione non deve essere condiviso con altri, od installato su più stazioni, se non esplicitamente previsto dalle licenze d'uso.
12. Lo sviluppo di software, da parte dell'unità organizzativa che ha in carico la stazione di lavoro, deve sottostare a procedure che prevedano le modalità di autorizzazione, preparazione, collaudo, modifica e di documentazione del prodotto sviluppato.
13. Ogni personal computer deve essere dotato di un prodotto anti-virus che venga attivato automaticamente alla sua accensione o secondo necessità.
14. E' vietato l'uso di unità esterne (pen drive, cd-ROM, DVD, ecc.) contenenti dati o programmi, tale divieto si applica anche ad unità provenienti da utenti esterni, a meno che non si tratti di Forze dell'Ordine in possesso di regolare mandato.

2.3.4. Area: protezione delle risorse. Accessi logici

Obiettivo: *rendere disponibili, in modo controllato, i dati e le applicazioni ed ogni altra risorsa informatica solo alle persone autorizzate e per motivi inerenti allo svolgimento del lavoro loro assegnato o in assolvimento a specifici obblighi contrattuali.*

Regole:

L'accesso alle risorse informatiche deve avvenire attraverso il processo di identificazione, quale l'associazione del codice utente e della password, o altra forma di riconoscimento inequivocabile (smart card, token, OTP, ecc.) e sulla base delle abilitazioni rilasciate.

L'accesso deve essere circoscritto ai soli dati/risorse autorizzati e viene concesso a:

1. dipendenti di ACI, in conformità alle esigenze derivanti dallo svolgimento del proprio lavoro;
2. personale di società esterne (consulenti, società collegate, società con interessi nel settore automobilistico, ecc.) limitatamente alle attività contemplate da appositi contratti di fornitura;
3. terzi appartenenti ad Organizzazioni convenzionate (Enti locali, Comandi di Polizia municipale, ecc.), limitatamente alle attività previste dalle convenzioni medesime;
4. soggetti che collaborano a vario titolo, per il tempo circoscritto alla durata dell'incarico ricevuto dall'Ente e limitatamente all'oggetto della collaborazione.

L'accesso deve essere autorizzato. L'autorizzazione viene richiesta dai Referenti dei dati e delle logiche operative (o loro delegati) per i dati e le applicazioni informatiche di competenza, e rilasciata, previa valutazione tecnica, dalla Direzione Sistemi Informativi e Innovazione.

L'autorizzazione viene revocata, su segnalazione del Referente dei dati, quando viene a cessare la necessità di disporre delle risorse/dati (ad esempio: modifica di mansioni, cessazione servizio, astensione dal servizio o non utilizzo delle credenziali di accesso per un periodo superiore ai sei mesi, ecc.); la revoca può avvenire d'ufficio, senza comunicazione all'interessato. La richiesta e la comunicazione delle autorizzazioni agli interessati devono avvenire per iscritto. La richiesta sarà effettuata a cura del responsabile dell'unità organizzativa competente, il quale ha l'obbligo di segnalare tempestivamente ogni modifica organizzativa che abbia un qualsiasi effetto sulle autorizzazioni rilasciate.

Il permanere della validità dell'autorizzazione deve essere verificato almeno una volta ogni sei mesi (ri-certificazione utenti).

Gli utenti esterni ad ACI che utilizzano risorse informatiche dell'Ente devono operare sotto la supervisione del personale competente.

Una password valida dovrà essere:

1. composta da un numero minimo di 8 caratteri, ovvero, nel caso in cui l'applicazione non lo consenta, da un numero di caratteri pari al massimo consentito;
2. non deve essere associata a niente di logico che sia interpretabile o riconoscibile da sconosciuti in quanto associabile a caratteristiche note del titolare;

3. priva di ripetizioni consecutive di caratteri, contenere indifferentemente maiuscole e minuscole, lettere e numeri, caratteri speciali;
4. non deve avere una durata illimitata, ma dovrà essere sostituita oltre che al primo utilizzo, ogni 90 gg. se posta a protezione di dati critici e almeno ogni sei mesi in tutti gli altri casi;
5. l'archivio delle password giacente nel sistema deve essere cifrato e chi vi potrà accedere dovrà essere autorizzato e dovrà restare traccia nel sistema di ogni ingresso in tale file;
6. la password viene trasmessa agli interessati secondo modalità di consegna diverse dipendenti dal contesto e dalla tecnologia disponibile. In genere user e password dovranno viaggiare su canali separati; laddove gli applicativi siano dotati di cambio pw obbligatorio al primo accesso, le credenziali di autenticazione potranno essere veicolate tramite canale unico.

Se l'amministratore del sistema può accedere al file che contiene in chiaro tutte le password, il sistema dovrà registrare in maniera non alterabile tutti gli accessi a quel *file system manager.*

L'accesso mediante VPN va considerato quale modalità residuale e per i soli casi in cui non sia possibile l'accesso secondo le modalità ordinarie (vale a dire mediante Horizon). Essendo una modalità straordinaria, la richiesta di apertura di una nuova VPN va inoltrata alla Direzione Sistemi Informativi e Innovazione e soggetta a specifica autorizzazione. Per l'accesso mediante VPN è necessaria l'autenticazione con doppio fattore.

2.3.5 Area: sicurezza logica. Crittografia

Obiettivo: *massimizzare la riservatezza e l'integrità dei dati particolarmente critici.*

Regole:

1. I dati particolarmente critici devono essere protetti attraverso strumenti di crittografia, tenendo conto delle loro caratteristiche e del luogo in cui vengono conservati.
2. Le chiavi di crittografia devono essere ben protette e conosciute solo dai due punti di codifica e decodifica: esse devono essere comunicate, conservate e gestite in modo controllato e protetto.
3. Le chiavi di crittografia devono essere periodicamente cambiate.
4. Potranno essere assegnate ad utenti interni ed esterni particolari tipi di connessioni (VPN) per consentire il collegamento al Sistema Informativo dell'Ente. Le connessioni ad utenti esterni saranno attivate a seguito di specifica richiesta e successiva autorizzazione da parte dell'Ufficio per l'Organizzazione Digitale. L'utente esterno riceverà le credenziali di autenticazione (in modalità sicura) unitamente alle norme di comportamento da adottare per l'utilizzo della connessione. Per l'accesso alle VPN è richiesta l'autenticazione con doppio fattore.

2.3.6. Area: utenti esterni ad ACI

Obiettivo: *far operare gli utenti esterni ad ACI nell'ambito delle regole di sicurezza adottate e sotto la supervisione di un responsabile di ACI.*

Regole:

1. Ogni utilizzo di risorse informatiche di ACI da parte di utenti esterni deve essere regolamentato da un apposito contratto di servizio, il quale preveda in modo esplicito i vincoli al rispetto delle regole di sicurezza.
2. Ogni utente deve operare sotto il controllo di un Referente di dati e di applicazioni, il quale deve:
    a. tenere un elenco aggiornato di questi utenti che, periodicamente, saranno comunicati alla Direzione Sistemi Informativi e Innovazione;
    b. rilasciare/revocare le autorizzazioni agli accessi logici ai dati;
    c. accertare che il loro operato sia conforme alle normative ed intervenire prontamente qualora si manifesti una irregolarità.
3. Il Direttore di ciascuna Struttura responsabile della erogazione di servizi di fornitura dati deve assicurarsi che nei contratti di servizio sia previsto:
    a. la sottoscrizione degli utenti a impegnarsi alla non divulgazione di informazioni acquisite durante la loro permanenza in ACI;
    b. che l'operato degli utenti sia conforme alle normative;
    c. che l'attività lavorativa dell'utente esterno sia esercitata, qualora sia possibile, in locali diversi dagli altri uffici.

2.3.7. Area: dispositivi mobili

Regole:

L'Ente, con l'adozione del sistema di posta elettronica Gmail, ha deciso di fornire ai propri dipendenti uno strumento evoluto di work collaboration e cloud computing, non circoscritto al solo utilizzo della posta elettronica. Le potenzialità della nuova piattaforma consentono infatti di perseguire l'obiettivo di promuovere l'attività di condivisione di idee, esperienze, informazioni e materiali per la gestione di casistiche e problematiche inerenti l'ambito lavorativo.

Attraverso i nuovi strumenti ogni dipendente ha anche la possibilità di pubblicare messaggi sotto forma di "post", caricare testi, immagini, contenuti audio e video e qualunque altro tipo di materiale di creazione originale o riprodotto ai fini e per gli effetti descritti nel seguente documento. Utilizzando i nuovi strumenti, il dipendente accetta in ogni sua parte le condizioni e i termini di utilizzo di seguito precisati. Nell'utilizzo degli strumenti di *work collaboration,* il dipendente deve attenersi alle seguenti regole generali dettate dall'Ente:

- Regolamento recante codici di comportamento dei dipendenti pubblici - DPR 16/04/2013, n. 62
- Codice di comportamento di Ente

In particolare i dipendenti devono attenersi alle seguenti indicazioni:

1. Non è consentito servirsi o dar modo ad altri di utilizzare le APP messe a disposizione dall'Ente per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.
2. Gli Utenti si impegnano, inoltre, a non pubblicare o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi in materia civile, penale ed amministrativa vigenti.
3. Non procedere all'invio massivo di mail non richieste (spam). La spedizione di qualsiasi forma di spam attraverso il servizio di posta fornito è proibita.
4. Non fare pubblicità a nessun tipo di prodotto o servizio e non pubblicizzare, trasmettere o altrimenti rendere disponibile qualsiasi tipo di software, programma, prodotto o servizio che viola il presente regolamento o la legge vigente.
5. Non è consentito utilizzare l'account aziendale per registrarsi nei cosiddetti APP Store (es. Play Store, Apple Store, Windows Store).
6. Non è consentito utilizzare l'account aziendale per registrarsi sui Social Media (es. Facebook, Twitter, Instagram). Lo stesso può essere utilizzato sulle risorse messe a disposizione dall'Ente (es.: Community, Siti Tematici, Cloud Aziendale).
7. Ai dipendenti è messa a disposizione un'area del Cloud Aziendale (es.: Drive), per l'archiviazione e la condivisione di contenuti ad uso lavorativo. Non è consentita la condivisione dei contenuti di tale spazio con utenti esterni all'Ente, salvo che per i soggetti indicati al paragrafo 2.3.4.
8. Per motivate esigenze organizzative è possibile richiedere una deroga ai punti 5, 6, e 7, indirizzando una richiesta al Direttore della Direzione Sistemi Informativi e Innovazione.
9. Le regole che riguardano la posta elettronica e Internet, per quanto applicabili, sono da ritenersi valide anche per l'utilizzo di tutti i dispositivi mobili (p.c. portatili, tablet, smartphone aziendali) assegnati a vario titolo ai dipendenti (telelavoro, reti territoriali, smart working, ecc.).
10. Per quanto riguarda gli smartphone è buona norma proteggerli con sistemi di inserimento pin e/o blocco schermo. Procedere ad eventuali back-up dei dati se necessario. Scaricare sempre gli aggiornamenti di sistema e delle App legate all'utilizzo della posta e dei browser utilizzati per la navigazione in Internet ma mai software di provenienza incerta.
11. Per esigenze di sicurezza, è vietato utilizzare gli account istituzionali per la registrazione su siti esterni, salvo che non sia necessaria per esigenze di servizio[3].
12. Qualora gli venga segnalato che le sue credenziali sono state riscontrate dal sistema di Threat Intelligence nel Dark Web su alcuni leaked database, è necessario che il Dipendente proceda immediatamente alla modifica delle credenziali di accesso alla posta aziendale ed al dominio.
13. Il reset delle credenziali per l'accesso alla casella mail compete di regola solo al suo titolare. La Direzione Sistemi Informativi e Innovazione procede a resettare la password solo su richiesta del titolare o per gravi motivi di sicurezza.

[3] V. art. 16 Codice di comportamento

3. Gestione della Sicurezza delle Informazioni e tutela della Privacy

3.1. Compiti istituzionali di Sicurezza delle informazioni e tutela della Privacy

Vengono di seguito individuate le figure organizzative di ACI cui sono assegnate responsabilità in materia di Sicurezza delle Informazioni e tutela della Privacy, e ne vengono precisati in dettaglio gli ambiti di azione, le responsabilità e i relativi compiti.

Questi ultimi sono stati definiti in modo da consentire una realizzazione coordinata, continua e controllata delle politiche aziendali.

Tali descrizioni potranno variare nel tempo in relazione alle modifiche che interverranno nella tecnologia adottata, nelle strategie e nell'assetto organizzativo dell'Ente.

3.1.1. Introduzione

La realizzazione delle misure di Sicurezza delle Informazioni e tutela della Privacy, in conformità alla politica adottata, richiede la partecipazione attiva di tutti i collaboratori, oltre che la presenza di appropriate strutture organizzative specialistiche che indirizzano e coordinano le iniziative. La presente sezione individua le responsabilità e assegna i compiti ai diversi livelli della Struttura organizzativa di ACI. Con particolare riguardo alla protezione dei Dati personali, il Regolamento (UE) 679/2016 (GDPR), recante disposizioni per la protezione dei Dati personali, stabilisce che ogni Organizzazione debba adottare e mettere in atto misure tecniche e organizzative adeguate a garantire e dimostrare che il trattamento dei Dati personali avvenga nel rispetto della normativa in materia a tutela dei diritti e delle libertà dell'Interessato.

In adempimento a quanto previsto nell'art. 2 quaterdecies del D.Lgs. 196/2003 (Codice privacy) – così come integrato dal D.Lgs. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR - l'ACI, in qualità di Titolare del trattamento dei Dati personali di sua competenza, con delibera Presidenziale n. 7960 del 2 aprile 2019 ha adottato un Organigramma Privacy articolato nei ruoli funzionali di: - Referente - Designato - Autorizzato

- i **Referenti** sono tutti i dirigenti, sia di prima che di seconda fascia. Ai fini privacy, ad essi sono equiparati i Professionisti;
- i **Designati** sono i titolari di una posizione organizzativa funzionale, centrale o territoriale;
- gli **Autorizzati** sono tutti i dipendenti che effettuano il trattamento dei dati personali.

Si rinvio, per la disciplina di dettaglio, alla Delibera del Presidente n. 7960/2019.

I principali compiti in materia di sicurezza sono assicurati dalle Strutture organizzative:

Direzione Sistemi Informativi e Innovazione	Responsabile della Sicurezza Informatica Ufficio per l'Organizzazione Digitale, nel cui ambito operano la Funzione Sicurezza e gli Specialisti DSII per la Sicurezza ICT negli Uffici Territoriali
Strutture centrali	Direttori Centrali Dirigenti degli Uffici, nell'ambito delle Direzioni/Servizi responsabili al trattamento automatizzato dei dati personali Responsabili di progetto
Strutture periferiche	Direttore Compartimentale Direttore Area Metropolitana Direttore Area Territoriale Responsabile Unità Territoriale
ACI Informatica	Responsabilità di gestione Responsabilità di progetto Sicurezza IT
Utente finale	Qualsiasi dipendente o terzo esterno che accede ai dati ed alle applicazioni

Di seguito sono precisati i compiti di dettaglio assegnati alle singole figure organizzative.

3.1.2. Direzione Sistemi Informativi e Innovazione

La Direzione Sistemi Informativi e Innovazione è l'unità organizzativa presso la quale è esercitata la Responsabilità della Sicurezza ICT.

3.1.2.1. Direttore Direzione Sistemi Informativi e Innovazione

L'Ente è il proprietario delle risorse informatiche (hardware e software) direttamente o per il tramite della società ACI Informatica SpA. Il Direttore della Direzione Sistemi Informativi e Innovazione le acquisisce direttamente o per mezzo della società e le mette a disposizione

dell'intero Ente, assicurando l'erogazione del servizio di elaborazione secondo le caratteristiche richieste e adottando tutte le misure necessarie alla sicurezza dei dati, secondo il modello di contratto di servizio in vigore tra le parti.

Il Direttore della Direzione Sistemi Informativi e Innovazione:

- promuove lo sviluppo coordinato e bilanciato delle misure di sicurezza dell'intero Sistema Informativo ACI formulando le politiche e le strategie attuative in materia informatica, gli indirizzi e gli standard operativi e di sicurezza, garantendone la diffusione ed accertandone l'efficace applicazione;
- autorizza in parte l'acquisizione delle risorse informatiche, direttamente o per il tramite di ACI Informatica SpA (compresi i pacchetti applicativi), di cui devono dotarsi le strutture di ACI;
- conosce il livello di riservatezza dei dati affidati in elaborazione ed assicura a tutte le strutture dell'Ente l'adozione dei meccanismi di protezione, controllo e verifica degli ambienti informatici per l'attivazione delle restrizioni richieste;
- definisce i requisiti di protezione, utilizzo e controllo che devono essere presenti nella proprie aree e fa acquisire gli strumenti di sicurezza;
- fa assicurare, per il tramite della Società ACI Informatica SpA, la continuità del servizio di elaborazione.

3.1.2.2. Responsabile della Sicurezza Informatica

Il Responsabile della Sicurezza Informatica, nominato con delibera del Titolare, è il referente ACI per le strutture pubbliche deputate alla Sicurezza Nazionale (CERT – Computer Emergency Response Team) e deve:

- assicurare la corretta applicazione delle norme dell'Ente in materia di sicurezza delle informazioni;
- individuare la presenza di punti di debolezza e coordinare i piani di azione necessari alla copertura dei rischi informatici;
- collaborare con le altre strutture aziendali al fine di garantire la realizzazione di un ambiente informatico sicuro;
- adempiere agli atti formali previsti dalle norme quali la stesura del presente documento;

Il Responsabile della Sicurezza per l'espletamento dei compiti propri dell'incarico si avvale dell'Ufficio per l'Organizzazione Digitale, al cui interno opera l'area denominata Funzione Sicurezza.

L'Ufficio per l'Organizzazione Digitale, avvalendosi della Funzione Sicurezza, assicura i seguenti adempimenti:

1. fornire supporto al Responsabile della Sicurezza nella formulazione delle regole di sicurezza, assicurando coerenza con le caratteristiche dei sistemi di controllo interno e la copertura dei potenziali rischi informatici;

2. fornire, su richiesta, supporto ai responsabili di progetti ACI nella stesura dei documenti di analisi dei requisiti in materia di sicurezza per lo sviluppo o le modifiche significative di applicazioni informatiche;
3. assicurare, su richiesta specifica, che le attività di collaudo comprendano anche l'analisi degli aspetti connessi alla sicurezza e che gli stessi siano correttamente trattati nel manuale utente;
4. condurre verifiche rivolte ad accertare l'efficace funzionamento dei meccanismi di sicurezza messi in atto;
5. proporre gli standard minimi di protezione, controllo e verifica che dovranno essere sempre rispettati;
6. definire i criteri di classificazione delle informazioni e le procedure per la loro attuazione;
7. costituire il punto di riferimento per tutte le strutture dell'ACI in materia di sicurezza, alle quali fornire guida e supporto per tutti gli aspetti connessi con la protezione ed il controllo degli ambienti e delle informazioni di competenza;
8. mettere in atto adeguati sistemi di controllo per la corretta gestione dei programmi di sicurezza e per il mantenimento dei livelli raggiunti nelle diverse aree aziendali; individuare le aree di rischio, accertare l'efficacia delle protezioni in atto e avviare la procedura di accettazione dei rischi;
9. analizzare le carenze segnalate e gli incidenti di sicurezza, congiuntamente alla società ACI Informatica SpA, e adoperarsi per far intraprendere dalle unità operative interessate le opportune azioni correttive;
10. accertare che le procedure di individuazione, valutazione ed accettazione dei rischi nelle unità operative siano gestite in modo corretto, tenendo informato il Direttore della Direzione Sistemi Informativi e Innovazione delle evoluzioni delle criticità riscontrate.

L'Uffico per l'Organizzazione Digitale può svolgere anche i seguenti compiti:

1. promuovere verifiche dello stato della Sicurezza delle Informazioni sulla base delle valutazioni dei rischi effettuate con le Direzioni responsabili, consolidandone i risultati;
2. verificare che le normative, gli standard, i piani e le misure di sicurezza trovino effettivo riscontro nella operatività quotidiana;
3. svolgere attività di verifica sull'efficacia del controllo degli accessi ai sistemi informatici; accerta la legittimità delle operazioni e rileva eventuali violazioni;
4. verificare l'adeguatezza delle procedure e dei piani di ripristino delle attività in caso di "disastro";
5. tenere informato il Responsabile della Sicurezza Informatica circa le criticità riscontrate e l'efficacia delle azioni intraprese.

L'Ufficio per l'Organizzazione Digitale ha inoltre il compito di monitorare, per il tramite di Aci Informatica, i rischi provenienti in vario modo da attacchi dall'esterno.

Tra i suoi compiti, quello di diffondere la cultura della sicurezza e di elevare la sensibilità dei Dipendenti sulla esigenza di evitare comportamenti che possano inavvertitamente mettere a rischio la sicurezza, e di incentivare i comportamente invece virtuosi.

L'Ufficio per l'Organizzazione Digitale presidia la casella *cybersecurity@aci.it*, alla quale tutti i Dipendenti possono segnalare le mail di provenienza sospetta e ogni evento di si sospetta possa mettere a rischio la sicurezza.

3.1.3. Direzioni/Servizi Centrali

Il Direttore Centrale è responsabile della Struttura che gestisce i dati e al cui supporto le applicazioni sono destinate.

A questa figura spetta pertanto il compito di individuazione delle responsabilità, in termini di censimento delle informazioni; di modalità operative di trattamento dei dati; di attribuzione dei vari livelli di autorizzazione per l'accesso alle funzioni delle procedure, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni registrate.

Il Direttore Centrale dà disposizioni affinché:

1. i dati vengano distribuiti ed usati solo da persone che ne abbiano effettiva necessità nella conduzione della propria attività lavorativa, adottando un processo di autorizzazione per l'utilizzo dei dati di competenza;
2. ai dati ed alle applicazioni sia assegnata la giusta classificazione e il relativo livello di protezione;
3. siano individuati, valutati ed eventualmente accettati i rischi con la predisposizione di eventuali piani di emergenza;
4. siano adottate le azioni necessarie alla salvaguardia dei diritti di ACI, dei dipendenti, e per consentire l'assolvimento degli impegni assunti verso terzi;
5. siano opportunamente conservati i documenti e i supporti informatici per gli eventuali fini legali, fiscali ed operativi. Per facilitare l'adozione ed il continuo rispetto delle normative di sicurezza e mantenere sempre attivo un approccio positivo alla sicurezza, il Direttore Centrale si avvale della Direzione Sistemi Informativi e Innovazione per:
    a. fornire a Dirigenti e Funzionari della Direzione ogni guida e supporto per gli aspetti inerenti la protezione ed il controllo degli ambienti e delle informazioni; assisterli nella definizione del livello di riservatezza dei dati e dei documenti, dei metodi di conservazione, nonché nella individuazione dei documenti, dati o programmi vitali;
    b. curare che le guide, le istruzioni e gli standard in materia di sicurezza siano conosciuti e correttamente interpretati da tutto il personale della Direzione, avendo come riferimento le normative aziendali; emettere procedure e/o guide integrative e standard operativi al fine di assicurare la verificabilità degli ambienti e meglio specificare indirizzi in materia di protezione e controllo;
    c. sulla base delle direttive aziendali e delle esigenze della Funzione di appartenenza, identificare le azioni e le iniziative necessarie a mantenere l'ambiente protetto e controllato;
    d. mettere in atto adeguati sistemi di controllo per la corretta gestione dei programmi di sicurezza, rilevare tempestivamente eventuali situazioni non in

linea con gli standard prefissati, valutarne i rischi ed attivarsi per la eliminazione delle esposizioni;

e. individuare le aree di rischio del servizio determinando l'efficacia delle protezioni in atto, ed avviare la procedura di accettazione dei rischi;
f. in caso di incidenti nel campo della protezione dei dati, della documentazione o in quello del sistema di controllo, fornire assistenza nella conduzione delle necessarie verifiche;
g. fornire accordo sulla completezza delle misure di protezione, controllo e verifica inserite nel progetto di sviluppo o di acquisto di nuove applicazioni;
h. accertare, ove richiesta, la validità delle soluzioni prima della loro installazione; promuovere riunioni di sensibilizzazione degli utenti finali delle applicazioni informatiche affinché siano tenuti aggiornati sulle problematiche della Sicurezza.

Infine, in qualità di Referente del trattamento dei dati personali, il Direttore Centrale è tenuto al rispetto delle previsioni del GDPR, nonché di quanto statuito dal Titolare in materia.

3.1.3.1. Dirigenti delle Direzioni/Servizi

Ai Dirigenti nell'ambito delle strutture cui sono preposti è affidata l'attivazione e il mantenimento della sicurezza nell'area di competenza.

Ad essi è richiesto di assicurare la protezione delle informazioni utilizzate, dell'integrità dei dati immessi nei sistemi, e del loro corretto utilizzo. In particolare a tali figure compete:

1. l'identificazione delle informazioni utilizzate;
2. la richiesta al Direttore Centrale (o suo delegato) dell'autorizzazione all'accesso individuale ai dati per i propri collaboratori; è ammessa delega scritta, da parte del Direttore Centrale per il rilascio delle autorizzazioni;
3. l'applicazione delle misure di sicurezza da parte dei propri collaboratori;
4. la sorveglianza sull'uso improprio dei dati;
5. l'attuazione e la promozione della cultura della sicurezza e del controllo nella propria unità organizzativa, in collaborazione con il personale della Direzione Sistemi Informativi e Innovazione.

Inoltre, in qualità di Referenti del trattamento dei dati personali, i Dirigenti sono tenuti al rispetto delle previsioni del GDPR, nonché di quanto statuito dal Titolare in materia.

3.1.4. Uffici territoriali

3.1.4.1. Direttore Compartimentale, Direttore di Area Metropolitana/Territoriale e Responsabile di Unità Territoriale / di Area Metropolitana

Promuove, nell'ambito delle proprie competenze, la completa attuazione delle misure di sicurezza informatica indicate dalle normative aziendali e la sensibilizzazione del personale; sorveglia sul corretto utilizzo locale delle risorse assegnate. Il suo compito primario consiste, quindi, nel prestare scrupolosa attenzione a che le risorse continuino a essere protette da accessi non autorizzati e siano adeguatamente custodite.

Pertanto:

1. cura che gli standard, le guide e le normative in materia di sicurezza siano conosciuti, osservati e correttamente interpretati da tutto il personale della propria struttura;
2. cura che i dati ed i documenti a supporto siano gestiti in modo controllato e tale da assicurare la loro protezione e conservazione;
3. attiva ogni misura utile a garantire la sicurezza fisica degli ambienti operativi;
4. assume la responsabilità della sicurezza fisica delle installazioni informatiche ricevute in dotazione e assicura il corretto funzionamento degli impianti tecnologici, attivando e gestendo il controllo degli accessi ai locali;
5. attiva le azioni più opportune per prevenire l'uso improprio o la perdita di dati;
6. autorizza gli accessi fisici ai locali per gli utenti esterni.

Inoltre, in qualità di Referenti e di Designati al trattamento dei dati personali, sono tenuti al rispetto delle previsioni del GDPR, nonché di quanto statuito dal Titolare in materia.

3.1.5. ACI Informatica

La società ACI Informatica:

- è il gestore delle risorse informatiche centrali e periferiche di ACI;
- amministra direttamente le risorse di base (hardware, software di base, applicativi e reti trasmissione dati), le applicazioni ed i sistemi di sicurezza logica adottati;
- ha la responsabilità di mantenere integre le risorse, proteggendole da accessi non autorizzati e custodendole unitamente ai dati e ai programmi applicativi.

Ai sensi dell'Accordo per il trattamento dei dati personali, sottoscritto in data 24 maggio u.s. con Protocollo PRES. SG.SD n. 2509/2018 del 7 giugno, è il Responsabile del trattamento automatizzato dei dati per tutti gli archivi dell'Ente. A questa figura sono assegnati i compiti di seguito indicati:

Responsabilità di gestione

1. adottare per le attività di competenza processi elaborativi e metodologie che permettano il governo e la trasparenza delle operazioni e che rispondano ai requisiti di sicurezza; a tal proposito, conserva, aggiorna e fornisce annualmente alla DSII l'elenco dei nominativi di quanti svolgono il ruolo di "amministratore di sistema",

corredato dalla specifica dei relativi ambiti di competenza e l'elenco analitico di tutte le attività svolte;
2. assicurare la continuità del servizio di elaborazione, promuovendo ogni azione utile alla rimozione degli ostacoli tecnici;
3. attivare le metodologie per la tempestiva rilevazione, analisi e soluzione dei problemi tecnici che si manifestano nella erogazione del servizio.

Responsabilità di progetto

1. definire i requisiti generali di sicurezza, con le Direzioni/Servizi Centrali ACI, responsabili per competenza, prima di avviare un progetto di realizzazione di procedure informatiche;
2. definire formalmente, ove previsto, in collaborazione con la Direzione Sistemi Informativi e Innovazione, in fase di analisi, i componenti e criteri di sicurezza che devono essere previsti nella realizzazione di progetti informatici applicativi;
3. verificare tramite collaudo, che i requisiti di Sicurezza richiesti siano effettivamente realizzati;
4. svolgere le attività di manutenzione delle risorse applicative mantenendo inalterate le caratteristiche di sicurezza: ogni modifica di queste caratteristiche dovrà essere segnalata a tutte le funzioni interessate;
5. in presenza di impedimenti al rispetto degli standard coinvolgere la Direzione Sistemi Informativi e Innovazione per la valutazione dei rischi e per l'individuazione delle azioni da intraprendere.

Sicurezza IT:

1. fornire supporto nella valutazione e scelta delle risorse (hardware, software e personale) necessarie alla realizzazione dei piani in materia di sicurezza logica e fisica di competenza;
2. fornire, periodicamente, la reportistica relativa all'efficacia dei prodotti anti spamming, antispyware, di intrusion detection e di qualsiasi altro prodotto venga utilizzato ai fini della prevenzione di danni informatici;
3. tenere aggiornata la mappa delle installazioni, compreso il software di base ed i software di sicurezza presenti;
4. tenere costantemente aggiornate le versioni software presenti su tutte le postazioni di lavoro (es.: sistema operativo, browser, antivirus, ecc.);
5. esaminare le proposte di nuove installazioni concorrendo alla definizione dei requisiti di protezione e controllo;
6. assumere il ruolo di "Amministratore" del sistema operativo e, in quanto tale, mantenere il controllo dei meccanismi tecnici, curandone l'aggiornamento ed assicurandone la completa protezione delle risorse logiche di competenza;
7. svolgere attività di controllo sulla efficacia dei prodotti software di sicurezza installati: in presenza di incidenti di sicurezza, fornire assistenza nella conduzione delle necessarie indagini;

8. collaborare con la Direzione Sistemi Informativi e Innovazione per la individuazione dei rischi, nella loro valutazione ed eventuale accettazione;
9. mettere a disposizione di ACI, laddove richiesto, i log che permettano la ricostruzione delle operazioni informatiche;
10. tenere tempestivamente informata la Direzione Sistemi Informativi e Innovazione riguardo eventuali minacce e incidenti informatici e, quindi, sulle conseguenti attività che si intendono intraprendere.

3.1.6. Utente finale

L'utente è una persona (dipendente o terzo esterno) che accede ai dati ed alle applicazioni, utilizzandone le informazioni. Ogni utente deve essere autorizzato all'accesso dai Direttori di riferimento o da Dirigenti espressamente delegati. Egli deve pertanto:

1. ottenere le autorizzazioni all'uso delle risorse informatiche, compresa l'autorizzazione all'accesso ai dati;
2. utilizzare le informazioni solo nel modo definito dalla Direzione competente e nei limiti stabiliti dai vertici dell'Ente;
3. adeguarsi a tutte le normative di sicurezza e di controllo stabilite.

L'utente è inoltre responsabile di:

4. utilizzare le risorse e i dati solo per attività inerenti le operazioni che gli sono state affidate e consentite;
5. mantenere la riservatezza dei dati di cui viene a conoscenza;
6. mantenere la riservatezza delle credenziali di accesso;
7. segnalare tempestivamente sospetti utilizzi anomali o lacune del sistema di controllo;
8. svolgere le necessarie azioni di custodia delle risorse e dei dati di cui è in possesso (come il personal computer, p.c. portatili, tablet, smartphone, i supporti rimovibili, ecc.);
9. segnalare al settore assistenza il malfunzionamento o il danneggiamento della stazione di lavoro o parti di essa.

4. Accesso alle applicazioni mediante la piattaforma VMware Horizon

L'estensione della modalità di lavoro agile in tutti gli Uffici dell'Ente è stata accompagnata e supportata dalla realizzazione di ACI Digital Workspace, un ambiente di lavoro virtuale unito alla dotazione per tutti i Dipendenti di più moderni dispositivi hardware, sia per l'ufficio che per lo smart working, nonché la "virtualizzazione delle applicazioni" mediante un'infrastruttura che consente alle postazioni di lavoro presenti in ciascuna sede degli Uffici Territoriali e degli Uffici Centrali di utilizzare, attraverso tecniche di virtualizzazione, applicazioni non fisicamente residenti presso le medesime postazioni, bensì presso i server centrali. Operativamente quest'ultima consiste nell'accesso alle applicazioni tramite la nota piattaforma Vmware Horizon.

VMware Horizon è la piattaforma scelta dal Sistema Informativo ACI per la virtualizzazione delle applicazioni. Con la virtualizzazione, le applicazioni non sono più fisicamente residenti nel computer del Dipendente, bensì nei server centrali dell'ACI. In tal modo ACI ha realizzato la propria Digital Workspace, un ambiente di lavoro virtuale a cui i Dipendenti accedono per l'appunto mediante la piattaforma Horizon.

Va infatti tenuto presente che la maggior parte delle applicazioni utilizzate dai Dipendenti ACI (analogamente a quanto accade in qualunque altro contesto aziendale pubblico o privato) sono raggiungibili tramite la intranet, vale a dire la rete aziendale privata di ACI.

Fanno eccezione i servizi Google resi disponibili ai Dipendenti ACI, a partire dalla posta elettronica Gmail (tra tutti, sicuramente il servizio Google più utilizzato da tutti i Dipendenti ACI), Drive, Calendar, Meet ecc., i quali sono invece tutti raggiungibili tramite la rete pubblica (Internet).

I Dipendenti possono accedere alle applicazioni che risiedono nella Intranet mediante la piattaforma VMware Horizon. Di conseguenza, Horizon deve essere utilizzato esclusivamente per le applicazioni virtualizzate e residenti nei server centrali. Non va al contrario di regola usato per le applicazioni raggiungibili tramite Internet.

Gli Uffici Territoriali, le Direzioni Compartimentali e la Sede Centrale con la sostituzione dell'HW sono contemporaneamente passate alla modalità della virtualizzazione dei dati e delle applicazioni.

Le applicazioni che devono necessariamente essere raggiunte tramite Horizon (per chi lavora dall'ufficio con il nuovo HW o che si collega dallo smart working o dal telelavoro) sono ad esempio Archiflow, HR Access, Lotus Notes (per i Dipendenti della Sede Centrale), SAP (tranne alcune categorie di Addetti della Sede Centrale che per esigenze tecniche accedono mediante VPN) nonché a tutte le applicazioni raggiungibili tramite il portale Centro Servizi, compresi ad esempio il Portale della Comunicazione Interna, la procedura SMVP ecc..

Va inoltre utilizzato per tutte le applicazioni PRA e Tasse (queste ultime a meno che non si tratti di applicazioni della Regione, qualora siano raggiungibili tramite Internet o con le modalità specifiche della singola Regione).

Al contrario va evitato di utilizzare Horizon:

- per effettuare videoconferenze mediante Meet (o con qualunque altra piattaforma);
- in generale per accedere a contenuti multimediali come youtube, moodle (per i corsi online) etc;
- per l'accesso ad alcune applicazioni di altre amministrazioni (ad esempio Gtart, il gestionale della Regione Toscana per la lavorazione delle Tasse automobilistiche) che di volta in volta verranno segnalate al personale coinvolto;
- per la navigazione in internet (mediante Chrome o un altro browser).

Il motivo per cui è raccomandato di utilizzare al di fuori di Horizon le applicazioni indicate in questo gruppo (in quanto accessibili mediante internet) è per evitare di appesantire, e di conseguenza rallentare, inutilmente il sistema e la lavorazione.

Per esigenze di sicurezza, sono inoltre stati adottati criteri restrittivi nella navigazione internet avviando il browser all'interno di Horizon. È pertanto possibile che un sito sia irraggiungibile dalla navigazione all'interno di Horizon, e sia invece raggiungibile da fuori Horizon.

Qualora per esigenze di servizio si abbia comunque la necessità di accedere ad un sito da Horizon (ad esempio nei casi in cui sia necessario caricare o scaricare documenti da lavorare con le altre applicazioni presenti su Horizon, oppure nei casi in cui a causa dell'accesso a tali siti sia frequente nel corso della giornata lavorativa e risulti quindi più agevole l'accesso direttamente da Horizon), il Direttore o il Responsabile della Struttura che ravvisi tale necessità da parte del proprio Personale, potrà fare richiesta motivata alla Direzione Sistemi Informativi e Innovazione di sbloccare l'accesso ad uno specifico sito da Horizon.

In casi eccezionali, valutati dalla Direzione Sistemi Informativi e Innovazione, è consentito a singoli Dipendenti di accedere alle applicazioni residenti nella Intranet tramite VPN anziché tramite la piattaforma VMware Horizon, da utilizzare limitatamente alle sole applicazioni non disponibili su Horizon.

Il ruolo centrale della piattaforma VMware Horizon ha reso necessario innalzare il livello di sicurezza, rafforzando il metodo di identificazione e autenticazione dell'utente che accede, tramite la virtualizzazione, ai servizi e alle applicazioni rese disponibili dal Sistema Informativo dell'Ente, mediante l'introduzione dell'"autenticazione a due fattori" o "strong authentication".

Tale esigenza prende atto dalla considerazione del momento storico, del contesto ambientale e di quello tecnologico in cui, con la diffusione del lavoro agile, è indubbiamente aumentato il perimetro di attacco ed il conseguente rischio cui ci si espone utilizzando gli strumenti elettronici.

Pertanto l'accesso prevederà un metodo di autenticazione più sicuro rispetto a quello già noto ed esercitato mediante login e password, poiché implica l'aggiunta di un ulteriore elemento costituito da un generatore OTP (One-time password, vale a dire una password valida per un solo accesso), reso disponibile in forma fisica mediante un apposito dispositivo oppure mediante app gratuita, scaricabile sul proprio smartphone.

4.1. Adempimenti nel caso di furto o smarrimento del token per la generazione dell'OTP di accesso ad Horizon

Lo smarrimento del dispositivo fisico che funge da token, con il conseguente rischio che possa venire utilizzato da terzi estranei per l'accesso non autorizzato alle applicazioni ed ai sistemi ACI, costituisce un evento particolarmente delicato che rende necessario l'attivazione delle necessarie contromisure nei tempi più rapidi possibili. Il token smarrito deve pertanto essere prontamente disabilitato e va presentata la denuncia di smarrimento.

Il Dipendente che si accorge di non avere più la disponibilità del token deve anzitutto procedere alla sua disabilitazione.

Per ogni esigenza, il dipendente potrà comunque avvalersi del supporto del Referente Territoriale DSII (se assegnato ad un Ufficio PRA o ad una Direzione Compartimentale) oppure al Presidio Tecnico di Aci Informatica (se assegnato alla Sede Centrale), in modo che possa essere subito disattivato e non non ci sia il rischio che possa più essere utilizzato da terzi non autorizzati per l'accesso ad Horizon.

Il Dipendente deve inoltre avere cura di presentare nei tempi più rapidi denuncia di smarrimento alle Forze dell'Ordine.

La denuncia consegnata dal Dipendente andrà protocollata indicando come mittente il medesimo Dipendente che la presenta. In particolare, gli Uffici PRA protocolleranno la denuncia con la classificazione: DIREZIONE / SEGNALAZIONI AUTORITA' PS.

Le Strutture della Sede Centrale e delle Direzioni Compartimentali potranno invece protocollarla con la classificazione presente nel loro rispettivo titolario, corrispondente o comunque più simile a quella sopra indicata per gli Uffici PRA.

La denuncia andrà quindi conservata agli atti dell'Ufficio.

5. Regole tecniche per l'utilizzo della Posta elettronica e di Internet

Il presente capitolo contiene le regole tecniche di utilizzo della posta elettronica e di Internet, approvate dal Comitato Esecutivo dell'ACI in data 12 Settembre 2008 e successive modificazioni. Modifiche di carattere tecnico al presente capitolo possono essere apportate dal Responsabile della Sicurezza Informatica.

5.1 La navigazione in Internet

Regole tecniche:

La navigazione in Internet è permessa dalle stazioni di lavoro secondo le modalità del tipo di connessione utilizzato e con le misure di protezione previste per la rete aziendale (proxy server e/o strumenti di firewall software e hardware e antivirus).

L'accesso a Internet è consentito a tutti gli utenti attraverso un profilo "standard" di autorizzazione che consente anche l'utilizzo della propria cartella personale dei documenti e del software previsto per ogni postazione (cartella utilità) e la navigazione in ambiente intranet aziendale, laddove non siano previsti ulteriori particolari credenziali di autenticazione come ad esempio la posta elettronica.

Gli accessi ad Internet attraverso la rete aziendale sono sottoposti, per motivi di sicurezza, al controllo previsto dagli strumenti di firewall; essi sono registrati, monitorati e sottoposti a verifiche periodiche. Le verifiche devono essere limitate e riportate esclusivamente in forma di analisi statistiche semestrali non nominative a meno di esigenze determinate da segnali di particolare pericolosità per i beni aziendali come di seguito indicato.

Ogni volta che naviga un sito l'utente deve controllare sulla barra degli indirizzi la presenza o meno dell'icona del lucchetto, se presente significa che il sito è sicuro perchè sta utilizzando il protocollo HTTPS per comunicare. Può essere in ogni caso un sito Fake anche se usa protocollo HTTPS, è buona norma quindi controllare sempre anche la validità del certificato, cliccando sul lucchetto ed espandendo poi le informazioni sul certificato stesso.

Qualora vengano ravvisati, durante le analisi statistiche di cui sopra, traffici di pacchetti anomali o, in ogni caso, in grado di compromettere la sicurezza dei sistemi informativi, sarà inviata, da parte della Direzione Sistemi Informativi e Innovazione, una segnalazione di anomalia alla macro-organizzazione interessata (Unità territoriale, Direzione Compartimentale, Direzione/Servizio Centrale); se dopo la segnalazione l'anomalia continuasse a persistere, i controlli successivi saranno progressivamente più stringenti e le segnalazioni più frequenti, fino ad arrivare a verifiche su base personale, secondo quanto previsto dal Disciplinare per l'utilizzo degli strumenti elettronici.

Gli archivi (dati, immagini), le informazioni ed i programmi ricavabili da Internet possono essere coperti da copyright: in tal caso gli utenti sono tenuti al rispetto delle regolamentazioni di riferimento e comunque non è permesso direttamente o indirettamente effettuare download di materiale disponibile in rete protetto da diritto d'autore.

Eventuali abbonamenti a pubblicazioni presenti sulla Rete devono essere autorizzati e sottoscritti dal Responsabile dell'Ufficio di appartenenza dell'interessato o dal Direttore ed inoltrati per le necessarie verifiche di sicurezza alla Direzione Sistemi Informativi e Innovazione.

È consentita la partecipazione a corsi on line (Webinar, ecc.) previa autorizzazione del Direttore/Dirigente del proprio ufficio di appartenenza.

Può accadere che alcuni siti contengano virus; vanno osservati, pertanto, gli standard di sicurezza segnalati nelle Politiche di Sicurezza per la protezione delle stazioni di lavoro.

La registrazione a siti internet che non attengono allo svolgimento delle attività assegnate non è consentita. È comunque vietato l'uso dell'account di servizio per la registrazione su siti esterni e liste di distribuzione, salvo si tratti di siti il cui accesso è necessario per esigenze di servizio.

Non sono consentite attività on line di transazioni finanziarie, acquisti, aste on line e simili se non legate a funzioni di ufficio.

Non è consentito utilizzare siti esterni (cloud, area Internet) per memorizzare documentazione dell'Ufficio se non espressamente autorizzati.

Gli utenti non devono appesantire il traffico di rete con collegamenti particolarmente lunghi (download di file, connessioni a siti audio/video, connessioni peer to peer, chat, ecc.) se non per le normali attività lavorative.

L'Amministrazione si riserva di applicare profili di navigazione personalizzati per aree di appartenenza a seconda delle attività svolte e su questa base saranno autorizzati gli accessi, la navigazione, la registrazione a siti e l'eventuale download di dati o l'utilizzo di piattaforme audio/video).

L'Amministrazione si riserva di applicare restrizioni alla navigazione su siti Internet ritenuti inopportuni (social, chat, ecc.) per lo svolgimento delle attività lavorative attraverso la costituzione di black list (liste di siti non accessibili) con filtro dei contenuti che ne bloccano la fruizione audio/video.

L'utenza collegata a Google (Gmail) deve essere utilizzata per finalità istituzionali e l'uso personale è ammesso purchè contenuto in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

Agli utenti è fortemente sconsigliato l'uso della funzione *"salva password"* dei browser al fine di non memorizzare codici riservati nelle relative *cache*.

5.2 La posta elettronica

Regole tecniche:

Tutti i dipendenti ACI sono provvisti di una casella di posta elettronica con protocollo SMTP attivo verso l'esterno, rilasciata a fronte di un'identificazione del soggetto avvenuta attraverso la matricola e/o il codice fiscale. Tale casella deve essere utilizzata solo per finalità istituzionali.

Il dipendente utilizza la posta elettronica esclusivamente per fini di lavoro e per contattare le Organizzazioni sindacali rappresentative e le RSU della Struttura di appartenenza. Al dipendente non è consentito utilizzare la posta elettronica per usi impropri, quali l'invio di messaggi diffamatori, osceni, di profanazione, lettere minatorie o di offesa razziale, messaggi commerciali o di propaganda, le cosiddette "catene di S. Antonio", nonché l'utilizzo della posta elettronica con modalità di forum[4].

L'utente è responsabile della propria casella di posta elettronica nonché delle proprie credenziali di accesso alla casella.

Il sistema di Posta elettronica utilizzato è Gmail è l'accesso alla casella postale avviene attraverso l'inserimento di specifiche credenziali di autenticazione, conformi ai criteri minimi di sicurezza previsti dalla Legge. L'applicativo di Posta elettronica utilizzato in ACI è presente su tutti i posti di lavoro. Il dominio di posta esteso è "aci.it".

Il sistema di posta Gmail utilizza una piattaforma cloud ed è pertanto raggiungibile dall'utente via web.

L'account di posta elettronica è nominativo e generalmente coincide con <iniziale nome>. <cognome>, a meno di omonimie, esclusi simboli speciali (apostrofi e/o accenti). Per particolari esigenze organizzative possono essere consentiti account generici; in tal caso, è necessario che per tutto il tempo di validità dell'account di posta elettronica, sia indicato alla Direzione Sistemi Informativi e Innovazione il responsabile di riferimento a presidio della mailbox; la sua identificazione, come quella degli altri aventi diritto ad accedere alla casella di posta avviene attraverso matricola e/o password.

Vengono utilizzate caselle di posta istituzionale, anche Certificate, che fanno riferimento agli Uffici o a singoli servizi degli stessi (es. *unita.territoriale.aci.provincia@aci.it, urpprovincia@aci.it,* ecc.). L'accesso a tali caselle è consentito agli utenti autorizzati dai responsabili degli Uffici di appartenenza attraverso formale richiesta alla Direzione Sistemi Informativi e Innovazione. Gli utenti autorizzati sono deputati alla gestione (puntuale lettura, smistamento, verifica della funzionalità e richiedere gli eventuali necessari interventi di ripristino delle funzionalità, ecc.) di tali caselle.

In caso di caselle mail condivise l'accesso è consentito solo tramite delega dalla propria casella mail. Non è consentito l'accesso diretto tramite username e password a caselle mail condivise.

Ciascun messaggio inviato deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile[5].

[4] V. art. 13 Codice di comportamento
[5] V. art. 16 Codice di comportamento

Non è consentita, sotto dominio ACI, la creazione di un account di posta elettronica per utenti appartenenti ad entità esterne all'Ente, a meno che non si tratti di utenze provvisorie di durata definita create per il raggiungimento di particolari finalità dell'Ente (stagisti, collaboratori, ecc.); in tal caso, l'identificazione dell'utente avverrà tramite codice fiscale. Fanno eccezione le mailbox di società partecipate da ACI o comunque di Enti, Organismi e società ad ACI collegate per le quali è consentito utilizzare un dominio di terzo livello (es. informatica.aci.it; progei.aci.it; delegazioni.aci.it, ecc.).

L'invio di file allegati alla posta elettronica è commisurato alla capacità delle infrastrutture adottate, al fine di non causare l'indisponibilità dei sistemi e dei dati. Tali limiti possono essere variati dalla Direzione Sistemi Informativi e Innovazione a seguito di mutate condizioni tecnologiche.

In caso di assenza programmata e prolungata del titolare della casella di posta, è raccomandato di inserire previamente un messaggio di risposta in automatico utilizzando il Risponditore automatico di Gmail.

L'accesso alla postazione di lavoro e più in generale l'accesso ai messaggi di posta contenuti in una mailbox personale può essere delegato in via preventiva, secondo quanto previsto dal Disciplinare, ad altro dipendente ("fiduciario") in caso di assenza improvvisa e prolungata e per improrogabili necessità legate all'attività lavorativa; in caso di mancata nomina del fiduciario, il dirigente di riferimento riveste d'ufficio l'incarico di fiduciario; il fiduciario è in ogni caso obbligato a richiedere autorizzazione di accesso alla Direzione Sistemi Informativi e Innovazione che, vagliata positivamente l'opportunità della richiesta disporrà, attraverso l'Amministratore di sistema, il reset delle credenziali per il tempo strettamente necessario ad effettuare la consultazione del caso; l'Amministratore provvederà anche alla generazione di nuove credenziali (da comunicarsi al dipendente all'atto del rientro in servizio) terminate le operazioni descritte.

E' altamente sconsigliato l'accesso da computer pubblici (es. computer di hotel, bar, e simili) al proprio account Gmail fornito dall'Ente, nonchè agli strumenti ad esso correlati di work collaboration e cloud computing, qualora non sia possibile derogare tale utilizzo, si raccomanda di terminare la sessione utente da Google workspace alla conclusione del lavoro e di rimuovere tutti i dati eventualmente scaricati sul computer pubblico..

Ogni messaggio inviato all'esterno dell'Amministrazione riporta in calce la seguente comunicazione (ripetuta in lingua inglese): *"La presente comunicazione è inviata dall'Automobile Club d'Italia. Gli eventuali dati da Lei forniti verranno utilizzati per comunicare esclusivamente con Lei e non verranno portati a conoscenza di terzi ma, ove necessario, comunicati all'interno della nostra Amministrazione. Nel caso invece la presente comunicazione Le fosse pervenuta per errore, La informiamo che la sua diffusione e riproduzione è contraria alla Legge e La preghiamo di darcene prontamente avviso e di cancellare quanto ricevuto".*

L'account di posta, non appena il titolare abbia, per qualsiasi ragione, terminato il proprio rapporto di lavoro con ACI, sarà dismesso nel più breve tempo possibile e comunque entro e non oltre un mese dalla risoluzione del rapporto.

Il dipendente (prima della data di cessazione) può inserire un messaggio automatico che avvisi che la casella non è più presidiata e che inviti a scrivere (per le comunicazioni di servizio) ad una diversa casella individuata in accordo con il Responsabile della Struttura di appartenenza, ed eventualmente anche ad una casella personale (non di servizio) per le eventuali comunicazioni di carattere personale. Dopo 30 giorni, la casella viene definitivamente dismessa e non verranno più recapitati messaggi automatici. Su richiesta del dipendente, è consentito scaricare i messaggi della casella prima della disattivazione, per poterli conservare su un proprio dispositivo locale.

In caso di mancata consegna di un messaggio di posta elettronica, al mittente viene comunicata dal router di posta la specifica tecnica dell'anomalia.

I messaggi di posta elettronica residenti sui server aziendali saranno conservati a tempo indeterminato, se non cancellati o archiviati in sede locale dall'utente; il personale deve pertanto periodicamente eliminare i messaggi privi di particolare rilevanza e, comunque, preventivamente in caso di risoluzione del rapporto di lavoro.

Non è consentito utilizzare tecniche di spam (invio massiccio di comunicazioni) o inoltrare posta sotto forma di "catene di Sant'Antonio" o diffondere messaggi di provenienza dubbia.

Il dipendente è responsabile del contenuto dei messaggi inviati, pertanto pone particolare attenzione affinché i messaggi di posta elettronica che invia, all'interno o all'esterno dell'Amministrazione, non siano oltraggiosi, discriminatori o possano essere in qualunque modo fonte di responsabilità della stessa Amministrazione.[6]

Invii di messaggi di posta a liste di distribuzione interne possono essere regolamentate da specifiche disposizioni di servizio.

È fatto divieto di trasmettere a chiunque a mezzo Posta elettronica documenti dell'Ufficio se non autorizzati o comunque nell'ambito delle finalità istituzionali.

Deve essere prestata la massima attenzione ogni volta che riceve una mail, deve essere verificato che l'email sia autentica, controllare il mittente e fare attenzione nel cliccare su eventuali link o allegati.

Non devono essere mai fornite informazioni sensibili tramite mail.

L'utente deve controllare l'URL del mittente verificando in particolare se contiene segnali che possano rendere sospetto il messaggio, quali:

- un dominio non correlato con l'azienda che ha inviato il messaggio
- errori ortografici
- simboli random
- simboli provenienti da altre lingue simili all'alfabeto latino.

Se, fatte le verifiche di cui ai punti precedenti, l'utente ritiene di essere di fronte ad una mail non sicura o dubbia, la stessa andrà inoltrata alla casella di posta cybersecurity@aci.it per le verifiche del caso.

[6] Art. 16 Codice di comportamento

6. Smartworking

Il presente capitolo contiene alcune raccomandazioni che i dipendenti devono adottare durante il lavoro agile al fine di utilizzare al meglio e in sicurezza i propri dispositivi. Tali raccomandazioni sono basate sul vademecum per lavorare on line in sicurezza di AGID.

Lo Smart Working, regolamentato dall'art. 14 della Legge 7 agosto 2015 n. 124, dalla legge del 22 maggio 2017 n. 81 e dal Decreto Legislativo del 9 aprile 2008 n. 81 è una modalità flessibile di esecuzione del rapporto subordinato. Pertanto la prestazione resa in modalità “agile” potrà avvenire in parte all’interno dei locali aziendali e in parte all’esterno, senza una postazione fissa, ed entro i soli limiti di durata massima dell’orario di lavoro giornaliero e settimanale (l’Amministrazione ha fornito a tutti i dipendenti, in comodato d’uso (secondo la disciplina di cui all’Art. 1803 e succ. C.C.) la strumentazione informatica idonea alle esigenze dell’attività lavorativa, nel rispetto delle norme di sicurezza vigenti.

Con l’Informativa sulla salute e sicurezza nel lavoro agile resa ai sensi dell’art. 22, comma 1, l. 81/2017 è stato precisato l’obbligo per il Dipendente in smart working di segnalare immediatamente al datore di lavoro, o al preposto le deficienze dei mezzi e dei dispositivi messi a loro disposizione, nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza.

L’utente in smart working è in particolare responsabile di:

1. utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;
2. effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;
3. assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati;
4. assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy descritta nel presente documento;
5. utilizzare l’accesso a connessioni Wi-Fi adeguatamente protette;
6. effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa.

Di norma il Dipendente svolge l’attività lavorativa in smart working utilizzando il computer portatile in dotazione. Si astiene di regola dall’accedere ai Sistemi ACI mediante propri dispositivi personali, salvo non ne sia stato autorizzato dal proprio Dirigente, sentita la Direzione Sistemi Informativi e Innovazione.

Il Dipendente che lavora in smart working deve avere cura di proteggere le informazioni accessibili tramite i dispositivi ed il software in dotazione allo scopo di evitare che, per mera disattenzione o per comportamento intenzionale da parte di eventuali terzi, le informazioni riservate del Sistema Informativo possano essere rese accessibili a terzi soggetti non autorizzati.

7. Politiche di sicurezza per il controllo degli accessi logici

7.1. Scopo del capitolo e campo di applicazione

Lo scopo del presente capitolo è quello di definire i princìpi, i ruoli, le responsabilità e le procedure da applicare per il controllo degli accessi logici ai sistemi informativi, alle reti di telecomunicazione, alle applicazioni informatiche e in generale alle informazioni in formato elettronico di ACI, al fine di ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati nonché la continuità dei servizi erogati. In particolare, obiettivo della presente politica è definire:

1. i princìpi generali di Information Security in ambito alla gestione degli accessi logici applicabili al contesto ACI;
2. i ruoli e le responsabilità connessi alla gestione degli accessi logici;
3. i criteri per l'assegnazione dei privilegi di accesso in modo coerente e controllato rispetto alle effettive esigenze degli utenti;
4. i criteri per il monitoraggio degli accessi a servizi di rete, applicativi, dati e per la tempestiva rilevazione di violazioni in materia di Information Security;
5. i criteri per il monitoraggio e l'aggiornamento periodico delle politiche di accesso.

La presente policy si applica a tutti i sistemi informativi, alle reti di telecomunicazione, alle applicazioni informatiche e in generale alle informazioni in formato elettronico e infrastrutture IT che supportano i processi di ACI. Essa è rivolta a tutto il personale dipendente e tutti i collaboratori esterni che nello svolgimento della propria attività lavorativa accedono e utilizzano le risorse informatiche di ACI. Tutti i dipendenti e i collaboratori esterni sono tenuti alla scrupolosa osservanza delle disposizioni in essa contenute al fine di garantire e tutelare il patrimonio informativo e ad adottare comportamenti conformi a quanto stabilito nel presente regolamento.

Il mancato rispetto o la violazione delle regole in esso indicate è perseguibile con provvedimenti disciplinari e, qualora si configuri come *reato informatico*, ai sensi della Legge 547 del 1993, recante modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica.

In particolare, anche in ambito controllo degli accessi logici sono applicabili gli artt. 615-ter e 615-quater del codice penale.

L'articolo 615-ter c.p. in particolare riguarda l'accesso abusivo a un sistema informatico o telematico. Tale reato si sostanzia nella condotta di colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. La pena prevista è quella della reclusione fino a tre anni. Secondo la giurisprudenza della Corte di Cassazione, commette il reato in esame colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso.

L'articolo 615-quater c.p. riguarda invece la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. Tale reato è punito con la reclusione sino a un anno e con la multa sino a 5.164 euro ed è commesso da chi - al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno - abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

7.2. Normative di riferimento

La presente Policy recepisce le best practice e gli standard nazionali ed europei applicabili al contesto, e in particolare:

- ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information security management systems requirements;
- ISO/IEC 27002:2013 – Information Technology – Security Techniques – Code of practice for information security controls;
- Circolare AgID n. 1/2017 del 17 marzo 2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Regolamento (UE) 679/2016 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR);
- D.Lgs. 193/2003 (Codice Privacy) così come modificato dal D. Lgs. n. 101/2017.

7.3. Tipologie di utenze

Dato il crescente quadro normativo di riferimento (tutela dei dati personali, responsabilità amministrativa, ecc.) che richiede precise responsabilità, anche individuali, nel trattamento delle informazioni e nell'utilizzo di sistemi e/o applicazioni, le politiche di sicurezza descritte individuano l'associazione di responsabilità collegate all'utilizzo di Utenze (che sono, in ultima analisi, responsabili dei vari accessi alle risorse informatiche). In ACI, in particolare, sono in uso le seguenti tipologie di utenze:

- Utenze di Dominio
- Utenze di Posta Elettronica
- Utenze di Posta Elettronica Certificata
- Utenze VPN (Virtual Private Network)
- Utenze applicative Centro Servizi
- Utenze altri applicativi
- Utenze di servizio

7.3.1. Utenze di Dominio

Tali utenze sono di norma assegnate a tutti i dipendenti ACI e consentono l'accesso alla dotazione informatica assegnata e agli strumenti informatici comuni, quali rete Internet, aree e cartelle condivise, stampanti di rete, ecc.

7.3.2. Utenze di Posta Elettronica

Tali utenze consentono l'accesso ai servizi di Posta Elettronica aziendali. In tale ambito è possibile distinguere utenze nominali, assegnate a ciascun dipendente ACI, e utenze istituzionali, assegnate a Direzioni o Delegazioni per finalità di servizio e comunicazione con la clientela.

7.3.3. Utenze di Posta Elettronica Certificata

Tali utenze consentono l'accesso ai servizi di Posta Elettronica Certificata (PEC) e sono assegnate a un sottoinsieme ristretto e controllato di utenti:

- a ciascuna Direzione ACI è assegnata una casella PEC istituzionale;
- a ciascun Responsabile Unico di Procedimento è assegnata una casella PEC nominale;
- ciascuna Delegazione ACI ha facoltà di richiedere ad ACI Informatica SpA l'assegnazione di una casella PEC istituzionale.

7.3.4. Utenze VPN (Virtual Private Network)

Tali utenze consentono l'accesso remoto alla rete privata ACI sfruttando, come tecnologia di trasporto, il protocollo di trasmissione pubblico e condiviso della rete Internet. L'assegnazione di questa tipologia di utenze è strettamente ristretta e controllata. Esse possono far capo a:

1. Automobile Club provinciali;
2. agenzie automobilistiche locali convenzionate con ACI;
3. Delegazioni ACI che, per vincoli tecnici, non dispongono di connettività diretta alla rete ACI;
4. responsabili delle Direzioni Centrali di ACI;
5. società esterne che collaborano con la Direzione Sport Automobilistico per l'organizzazione di eventi sul territorio;
6. società esterne che mantengono rapporti diretti con l'Area Professionale Legale;
7. personale che svolge la prestazione lavorativa in telelavoro.

Dal punto di vista gestionale, è possibile identificare due tipologie di Utenze VPN in utilizzo in ACI:

- utenze afferenti a dipendenti ACI, per le quali il censimento e controllo avviene tramite i servizi di Dominio;

- utenze afferenti a soggetti esterni ad ACI, per le quali il censimento e controllo avviene tramite le funzionalità messe a disposizione dagli apparati di rete che erogano questo tipo di servizio (VPN Concentrator).

7.3.5. Utenze applicative Centro Servizi

Tali utenze consentono l'accesso agli applicativi e ai servizi ACI gestiti in maniera centralizzata tramite il portale "Centro Servizi". Tale portale implementa un sistema di controllo accessi di tipo RBAC (role based access control), che consente agli utenti di accedere, tramite un'unica autenticazione e sulla base del gruppo di appartenenza, esclusivamente alle risorse informatiche per le quali egli risulta specificatamente abilitato. In particolare, è possibile identificare:

1. Utenze afferenti a personale dipendente. In tale caso l'utenza eredita i privilegi di accesso del gruppo "Direzione" a cui il dipendente appartiene. Ulteriori attività di profilazione ad-hoc possono essere eseguite sulla base di richieste specifiche da parte della Direzione di appartenenza, motivate da effettive esigenze operative legate alle mansioni lavorative del dipendente.
2. Utenze afferenti a personale esterno. In tale caso l'utenza eredita i privilegi di accesso del gruppo "Contratto" a cui l'utente fa riferimento. Ulteriori attività di profilazione ad-hoc possono essere eseguite sulla base di richieste specifiche da parte del gestore ACI del contratto, motivate da effettive esigenze operative legate alle mansioni lavorative dell'utente nel perimetro del suddetto contratto.

7.3.6. Utenze altri applicativi

Tali utenze fanno riferimento ad applicativi che, a causa di vincoli tecnologici, gestionali, economici o di altra natura, non risultano integrati nel portale Centro Servizi. Tali applicativi includono, ad esempio:

l'applicativo utilizzato per la gestione di processi in ambito Risorse Umane, tra cui gestione paghe e produzione cedolini;

- il Protocollo informatico;
- la suite gestionale SAP;
- il Content Management System (CMS);
- l'applicativo BO Data Mart.

È pertanto compito delle suddette Direzioni garantire, per gli applicativi di propria responsabilità, la piena applicazione e il rispetto delle politiche di sicurezza definite all'interno del presente documento.

7.3.7. Utenze di servizio

Tale categoria include tutte le utenze necessarie per l'amministrazione ordinaria e straordinaria dei sistemi informativi di ACI (e.g. applicazione patch, implementazione del change management, ripristino a seguito di eventuali interruzioni, monitoraggio e controllo, predisposizione delle autorizzazioni di accesso al sistema, ecc.). In generale, tali utenze possono essere di tipo:

- sistemistico, ovvero utenze utilizzate dai sistemisti per l'amministrazione di server Windows, Unix, apparati di rete, appliance di sicurezza, ecc.;
- DataBase, ovvero utenze utilizzate dai DataBase Administrator di ACI per l'amministrazione delle diverse basi dati presenti nell'Ente;
- applicative, ovvero utenze utilizzate dagli amministratori degli applicativi per la gestione degli stessi. Tali utenze, per loro stessa natura, rappresentano utenze di tipo amministrativo, poiché consentono l'esecuzione di funzionalità critiche sui sistemi informativi di ACI e l'accesso a dati particolari. Per tale motivo, l'assegnazione delle stesse è fortemente ristretta e controllata.

7.4. Principali ruoli e responsabilità

Le attività di gestione degli accessi logici ai sistemi informativi aziendali di ACI prevedono il coinvolgimento di diversi attori, attivati nelle modalità e nelle tempistiche più opportune, tra cui i principali risultano essere:

Direzione Risorse Umane e Organizzazione;

Direzioni ACI;

Direzione Sistemi Informativi e Innovazione

ACI Informatica;

Utente.

Per ciascuno di essi, nel presente capitolo vengono descritti i principali compiti e responsabilità in materia di Information Security in ambito al controllo degli accessi logici.

7.4.1. Direzione Risorse Umane e Organizzazione

La Direzione Risorse Umane e Organizzazione ha la responsabilità di:

1. comunicare tempestivamente alla Direzione Sistemi Informativi e Innovazione eventuali nuovi ingressi nell'Ente, al fine di garantire la conseguente attivazione delle relative abilitazioni;
2. comunicare tempestivamente alla Direzione Sistemi Informativi e Innovazione tutte le evoluzioni afferenti al personale ACI (cambi di ruolo o mansione lavorativa,

distaccamenti, telelavoristi, ecc.) che possano comportare la necessità di adeguare rapidamente il profilo informatico dei dipendenti impattati;
3. comunicare tempestivamente alla Direzione Sistemi Informativi e Innovazione interruzioni di rapporti di lavoro a vario titolo (e.g. licenziamenti, dimissioni, pensionamenti, ecc.), al fine di garantire la tempestiva cessazione delle relative utenze nei sistemi informativi di ACI.

7.4.2. Direzioni ACI

Le Direzioni ACI hanno la responsabilità di:

1. definire, per le applicazioni di cui risultano owner e di concerto con la Direzione Sistemi Informativi e Innovazione, regole appropriate per il controllo degli accessi logici al proprio servizio/applicazione, intese come l'insieme di privilegi e restrizioni associate a ciascun ruolo all'interno del servizio / applicazione, sulla base di un'analisi del rischio associato e in coerenza con i principi fondamentali di segregation of duties, need to know e least privilege;
2. richiedere la creazione di utenze e l'attribuzione di autorizzazioni afferenti a dipendenti e terze parti di propria responsabilità, sulla base delle effettive esigenze operative e utilizzando esclusivamente gli appositi canali e strumenti aziendali predisposti, che garantiscono la tracciatura di ciascuna richiesta;
3. comunicare tempestivamente alla Direzione Sistemi Informativi e Innovazione tutte le evoluzioni afferenti alle utenze / abilitazioni richieste (e.g. cambi di mansione, evoluzioni nelle esigenze operative, interruzione di contratti, ecc.) che possano richiedere la revisione delle abilitazioni concesse o la cessazione delle utenze create;
4. vigilare sul corretto utilizzo delle utenze e delle abilitazioni richieste, in conformità alle politiche definite nel presente documento e alla legislazione vigente.

7.4.3. Direzione Sistemi Informativi e Innovazione

La Direzione Sistemi Informativi e Innovazione è responsabile per:

1. assicurare la rispondenza del sistema informativo alle politiche di sicurezza e di tutela delle persone e di altri soggetti in relazione al trattamento automatizzato dei dati personali;
2. assicurare sotto il profilo gestionale il funzionamento dei servizi di accesso alle banche dati e/o di forniture di dati erogati dal sistema informativo ai soggetti terzi che ne abbiano interesse. In particolare, essa è responsabile per:
3. verificare che le regole per il controllo degli accessi logici ai servizi / applicazioni di ACI siano coerenti con i principi di segregation of duties, need to know e least privilege;
4. verificare la conformità delle richieste ricevute dai soggetti richiedenti rispetto alle politiche di sicurezza di ACI e alla legislazione vigente ed eventualmente autorizzarne l'esecuzione;
5. garantire il governo delle eventuali eccezioni / non conformità in ambito controllo degli accessi logici rispetto alle politiche di sicurezza di ACI (ad esempio a causa di

vincoli tecnologici, organizzativi, economici o di altra natura), valutando e monitorando il rischio per la sicurezza delle informazioni associato e definendo, ove necessario, opportuni controlli compensativi;
6. governare attivazione, modifica o disattivazione delle autorizzazioni sul Centro Servizi in conformità alle richieste ricevute e in coerenza con quanto stabilito dal presente documento e dalle altre politiche di sicurezza aziendali;
7. garantire la definizione e la continua adeguatezza delle politiche di sicurezza per il controllo degli accessi logici, in conformità agli standard e alle best practice di settore e alla legislazione vigente;
8. monitorare la corretta applicazione della presente politica.

7.4.4. ACI Informatica

ACI Informatica è responsabile per:

1. l'attivazione, modifica o disattivazione delle utenze e delle autorizzazioni di propria competenza, in conformità alle richieste e alle autorizzazioni ricevute e in coerenza con quanto stabilito dal presente documento e dalle altre politiche di sicurezza aziendali;
2. il monitoraggio, attraverso gli strumenti tecnologici a disposizione e nei limiti della legislazione vigente, del corretto utilizzo delle utenze e delle autorizzazioni fornite, con speciale riferimento alle utenze amministrative, e l'attivazione degli opportuni processi per la gestione di eventuali anomalie.

7.4.5. Utente

Ciascun utente è responsabile per:

- l'utilizzo delle proprie utenze e autorizzazioni di accesso logico a sistemi e applicazioni IT di ACI, in conformità alle prescrizioni definite nel presente documento, nelle Politiche di Sicurezza di ACI e in compliance alla legislazione vigente;
- segnalare prontamente alla Direzione Sistemi Informativi e Innovazione qualsiasi anomalia riscontrata, con particolare riferimento ad abilitazioni attribuitegli impropriamente o senza valida motivazione;
- adottare tutte le precauzioni a tutela del corretto funzionamento di sistemi e applicazioni IT e della sicurezza delle informazioni sensibili o di business accessibili / elaborate per loro tramite.

7.5. Politiche di sicurezza

Nel presente capitolo sono descritte le politiche di sicurezza che ACI ha definito per una corretta gestione dell'accesso logico ai sistemi informativi aziendali da parte di dipendenti e terze parti interessate. Tali politiche sono suddivise nelle seguenti tre categorie.

1. gestione del sistema di controllo degli accessi logici: politiche di sicurezza che devono essere applicate nella gestione del sistema di controllo degli accessi logici da parte delle strutture competenti;
2. responsabilità degli utenti: politiche di sicurezza che devono essere applicate dagli utenti dei sistemi e delle applicazioni;
3. controllo degli accessi ai sistemi e alle applicazioni: politiche di sicurezza che devono essere implementate all'interno di sistemi e applicazioni di ACI.

Nei paragrafi che seguono, si riportano le politiche di sicurezza afferenti alle categorie sopra descritte.

7.5.1. Gestione del sistema di controllo degli accessi logici

7.5.1.1. Principi fondamentali di sicurezza

Tutte le attività afferenti alla gestione del sistema di controllo degli accessi logici devono essere svolte in conformità ai seguenti principi fondamentali:

1. Principio della Necessità di Sapere (Need to Know), secondo cui i soggetti che devono compiere attività di trattamento di informazioni sono autorizzati a trattare i soli dati essenziali allo svolgimento dell'attività lavorativa.
2. Principio del Privilegio Minimo (Least Privilege), secondo cui a ciascun utente sono assegnate le sole abilitazioni strettamente necessarie allo svolgimento della propria attività lavorativa.
3. Principio della Segregazione dei Ruoli (Segregation of Duties), che mira a separare le attività / responsabilità relative ad un determinato processo aziendale, al fine di evitare la concentrazione di compiti critici nelle mani della stessa persona / Funzione, con lo scopo di ridurre il rischio di frode e accesso non autorizzato. In ambito controllo degli accessi logici, tale principio ha due impatti principali:
    a. il primo impatto riguarda il processo stesso di provisioning di utenze e privilegi, all'interno del quale le fasi di richiesta, autorizzazione e implementazione devono essere svolte da attori separati;
    b. il secondo impatto riguarda la gestione delle utenze applicative, alle quali non possono fare capo privilegi che permetterebbero di eseguire transazioni applicative incompatibili tra di loro (e.g. inserimento di fatture a sistema e autorizzazione al pagamento).

7.5.1.2. Registrazione e de-registrazione degli utenti

È necessario che sia attuato un processo formale di registrazione e de-registrazione per abilitare l'assegnazione delle utenze. Tale processo deve prevedere:

1. l'utilizzo di utenze univoche al fine di garantire l'identificabilità certa della persona fisica che ne fa uso; l'utilizzo di utenze condivise, pertanto, deve essere scoraggiato

e consentito, tramite approvazione formale e documentata della Direzione Sistemi Informativi e Innovazione, solo in caso di vincoli tecnici / operativi dimostrabili;
2. la disabilitazione o rimozione tempestiva di utenze afferenti a utenti, interni o esterni, che abbiano cessato il proprio rapporto di collaborazione con l'Ente;
3. l'identificazione periodica e la disabilitazione o rimozione delle utenze non più in uso; tali utenze non devono essere assegnate ad altri utenti neanche in tempi diversi.

7.5.1.3. Assegnazione e revoca dei privilegi

È necessario che sia attuato un processo formale per l'assegnazione o la revoca dei privilegi per tutte le tipologie di utenze e per tutti i sistemi e i servizi. Tale processo deve prevedere che:

1. la richiesta di assegnazione di un privilegio sia autorizzata da parte del Responsabile dell'applicazione o del servizio a cui fa riferimento;
2. la richiesta di assegnazione di un privilegio sia verificata, da parte della Direzione Sistemi Informativi e Innovazione, per assicurarne la conformità alle politiche di sicurezza di ACI e ai principi fondamentali di Need to Know, Least Privilege e Segregation of Duties;
3. l'assegnazione di privilegi a collaboratori o terze parti sia limitata nella durata al solo periodo strettamente necessario per lo svolgimento della prestazione correlata e sia fornita solo a fronte di accordi contrattuali e, ove necessario, non disclosure agreement;
4. i privilegi di accesso a sistemi e applicazioni non siano attivati prima del completamento del processo di autorizzazione;
5. sia mantenuto un archivio dei diritti di accesso assegnati a ciascuna utenza rispetto a ciascun servizio / applicazione;
6. i privilegi siano tempestivamente riesaminati per quegli utenti che abbiano cambiato ruolo o mansione lavorativa all'interno dell'Ente, e terminati per quegli utenti che abbiano cessato il proprio rapporto di collaborazione con ACI;
7. con speciale riferimento alle utenze VPN, le suddette devono essere autorizzate ad accedere ai soli segmenti di rete o singoli indirizzi IP relativi ai servizi a cui l'utente è stato autorizzato ad accedere.

7.5.1.4. Gestione dei privilegi amministrativi

In tale ambito, si richiamano le prescrizioni contenute nel provvedimento del Garante del 27 novembre 2008 – "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e della estensione delle responsabilità che a questa figura sono state attribuite con l'avvento del GDPR (Regolamento UE 679/2016):

1. l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il

quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
2. la designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
3. gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;
4. nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
5. l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
6. devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Si applicano, inoltre, le seguenti politiche di sicurezza definite da ACI:

7. i privilegi amministrativi devono essere assegnati a Utenze diverse da quelle utilizzate per le normali attività di business;
8. le Utenze con privilegi amministrativi non devono mai essere condivise, tranne che in condizioni di emergenza o di sussistenza di specifici vincoli tecnologici;
9. le Utenze con privilegi amministrativi devono essere di tipo strettamente personale e riconducibili a una persona fisica; qualora l'utilizzo di utenze generiche risulti indispensabile, devono essere adottati opportuni meccanismi finalizzati a:
10. garantire la segretezza delle informazioni di autenticazione condivise, ad esempio modificando la password periodicamente e ogni qualvolta un utente che ne sia a conoscenza termini il suo rapporto di collaborazione con ACI o cambi mansione lavorativa;
11. garantire la riconducibilità delle azioni effettuate dall'utenza generica a una persona fisica precisa (principio di accountability), ad esempio adottando meccanismi di password vaulting o escalation dei privilegi.

7.5.1.5. Gestione delle informazioni segrete di autenticazione

L'assegnazione di informazioni segrete di autenticazione deve essere controllata attraverso un processo di gestione formale, nello specifico:

1. agli utenti deve essere formalmente richiesto di tutelare la riservatezza delle informazioni segrete di autenticazione;
2. agli utenti devono essere inizialmente fornite informazioni segrete di autenticazione provvisorie, uniche e in compliance con le password policy di ACI, che debbano essere modificate al primo accesso;
3. le informazioni segrete di autenticazione provvisorie devono essere fornite agli utenti in modo sicuro, al fine di minimizzare il rischio di intercettazione da parte di terze parti (ad esempio tramite canali di comunicazione crittografati o busta cieca);
4. la procedura di assegnazione di informazioni segrete di autenticazione deve prevedere una conferma della corretta ricezione delle stesse da parte dell'utente;
5. devono essere stabilite procedure per la verifica dell'identità di un utente prima di fornire nuove informazioni segrete di autenticazione;
6. le informazioni segrete di autenticazione di default devono essere modificate in seguito all'installazione di software e sistemi.

7.5.1.6. Riesame periodico

I Responsabili delle applicazioni/servizi devono riesaminare a intervalli regolari le utenze e i privilegi autorizzati, per verificarne l'effettiva necessità e la continua conformità alle politiche di sicurezza di ACI. Nello specifico:

1. utenze e privilegi di ciascun utente devono essere sottoposti a riesame periodico, con cadenza almeno annuale, e in seguito a eventuali cambiamenti nel rapporto di lavoro con ACI (e.g. promozione, distacco, cessazione del rapporto di lavoro, ecc.);
2. deve essere eseguita una review periodica, con cadenza almeno trimestrale, degli account che presentano eccezioni di sicurezza, come ad esempio account bloccati, account con password scaduta, ecc.

7.5.1.7. Rimozione o modifica dei diritti di accesso

È necessario che i diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni siano rimossi al momento della cessazione del rapporto di lavoro / contratto, o che siano adattati ad ogni variazione. In particolare, deve essere stabilito un processo formale per la rimozione dei diritti di accesso che includa quanto segue:

1. le utenze devono essere revocate o disattivate al più presto possibile e in ogni caso non oltre dieci giorni in caso di dimissione del dipendente, risoluzione del contratto di lavoro. La disattivazione è immediata in caso di identificazione di una violazione della sicurezza;
2. tutte le informazioni segrete di autenticazione note all'utente impattato, con speciale riferimento a quelle condivise, devono essere modificate;
3. in caso di cambio di ruolo / mansione, le modifiche all'accesso devono riflettersi nella rimozione di tutti i privilegi non approvati per la nuova posizione;
4. le utenze cessate devono essere rimosse da qualsiasi tipo di gruppo o Access Control List.

7.5.1.8. Gestione dei diritti di accesso mediante Responsabile Operativo

Il Responsabile operativo è la persona fisica appartenente ad organizzazioni esterne all'Automobile Club d'Italia , dotato di una utenza privilegiata che gli consente di gestire, per conto di quest'ultimo, le utenze relative al personale che presta lavoro all'interno della propria organizzazione inerenti le autorizzazioni, i privilegi ed i diritti d'accesso ai dati ed ai servizi.

L'ACI individua le tipologie di organizzazione pubblica o privata, alle quali siano erogati servizi che comportino l'accesso al proprio Sistema Informativo, per le quali reputa opportuna la gestione delle utenze mediante il Responsabile operativo.

Nelle amministrazioni pubbliche il Responsabile operativo può coincidere con il Dirigente dell'Ufficio o delle Struttura, oppure può essere un dipendente assegnato al medesimo Ufficio o Struttura.

Nelle imprese private il Responsabile operativo può coincidere con il rappresentante legale, oppure con il preposto o institore o con altro soggetto avente una carica all'interno dell'impresa (es. consigliere). Può altresì essere un dipendente a tempo indeterminato dell'impresa.

L'Automobile Club d'Italia concede al Responsabile operativo di rilasciare, abilitare, disabilitare logicamente le utenze relative al personale che presta lavoro all'interno della propria organizzazione inerenti le autorizzazioni, i privilegi ed i diritti d'accesso ai dati ed ai servizi.

L'attribuzione del ruolo di Responsabile operativo costituisce una concessione unilaterale dell'ACI. Le funzioni concesse al Responsabile operativo possono essere revocate dall'ACI in qualunque momento e senza obbligo di motivazione.

L'ACI si riserva di avvalersi della facoltà di procedere direttamente all'abilitazione o disabilitazione dei singoli Operatori anche nei casi in cui sia stato già nominato il Responsabile operativo.

L'ACI può, in ogni caso ed a proprio insindacabile giudizio, procedere direttamente alla disabilitazione dei singoli Operatori già abilitati dal Responsabile operativo. Può inoltre, a proprio insindacabile giudizio, procedere alla disattivazione delle utenze che siano rimaste inutilizzate per un periodo minimo di sei mesi.

L'ACI definisce le modalità di rilascio delle credenziali e si riserva la facoltà di modificarle.

La designazione del Responsabile operativo compete, per i servizi erogati a Pubbliche amministrazioni, al Dirigente o Responsabile dell'Ufficio o della Struttura che si avvale dell'accesso al Sistema Informativo per la fruizione dei servizi ACI.

Per i servizi erogati a imprese private la designazione compete al rappresentante legale.

Il Dirigente o il Responsabile dell'Ufficio o della Struttura della pubblica amministrazione o il rappresentante legale dell'impresa inviano ad ACI la copia della nomina del Responsabile operativo, conferita utilizzando il modulo allegato.

L'ACI rilascia le credenziali al Responsabile operativo nominato dal Dirigente o dal Responsabile dell'Ufficio o della Struttura della pubblica amministrazione ovvero dal rappresentante legale dell'impresa previa verifica che il soggetto nominato abbia i requisiti indicati dal presente Disciplinare.

Il Responsabile operativo può essere identificato, alternativamente, mediante SPID o CIE nei casi in cui sia previsto l'accesso ai servizi con tale modalità. È altresì identificato mediante l'uso della firma digitale.

Nei casi in cui non sia previsto un accesso alle procedure che comportino l'identificazione con SPID e CIE nè utilizzi la firma digitale, Il Responsabile operativo è tenuto ad esibire o inviare in copia un documento di identità avente validità in Italia.

Non possono essere nominati Responsabile operativo coloro che:

- abbiano subito condanne penali per delitti contro la pubblica amministrazione o per i reati di cui agli artt. 615 ter (Accesso abusivo ad un sistema informatico o telematico), 615 quater (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici), 615 quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) del Codice penale;
- abbiano subito sanzioni previste dagli articoli 83 e 84 del Regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR);
- abbiano già avuto il ruolo di Responsabile Operativo e ne sia decaduto a seguito dell'accertamento di irregolarità.

Il Responsabile operativo può rilasciare, abilitare, disabilitare le utenze dopo aver verificato, sotto la propria responsabilità, il possesso dei seguenti requisiti da parte degli Operatori:
si tratti di una persona interna alla organizzazione, in particolare:

- per le amministrazioni pubbliche un dipendente assegnato al medesimo Ufficio o Struttura o appartenente ad una impresa che presti servizi sotto il diretto controllo dell'Ufficio o della Struttura;
- per le imprese private un soggetto avente una carica all'interno dell'impresa (es. preposto, institore, consigliere) oppure un dipendente a tempo determinato o indeterminato della medesima impresa;
- non abbiano subito condanne penali per delitti contro la pubblica amministrazione o per i reati di cui agli artt. 615 ter (Accesso abusivo ad un sistema informatico o telematico), 615 quater (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici), 615 quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) del Codice penale;

- non abbiano subito sanzioni previste dagli articoli 83 e 84 del Regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR).

Il Responsabile operativo deve ritenersi decaduto da ogni funzione e deve astenersi da ogni attività relativa alla rilascio, abilitazione e disabilitazione delle utenze in caso di:

- cessazione di ogni rapporto con l'organizzazione per conto della quale è stato nominato;
- abbia subito condanne penali per delitti contro la pubblica amministrazione o per i reati di cui agli artt. 615 ter (Accesso abusivo ad un sistema informatico o telematico), 615 quater (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici), 615 quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) del Codice penale;
- abbia subito una delle sanzioni previste dagli articoli 83 e 84 del Regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR).

In caso di sopravvenuta causa di cessazione, il Responsabile operativo è tenuto ad astenersi da ogni funzione e a darne immediata informativa al proprio Dirigente (se appartenente ad una Struttura pubblica) o al rappresentante legale (se appartenente ad una impresa privata). Il Dirigente o il rappresentante legale ne dà comunicazione all'ACI mediante PEC inviata alla casella di posta elettronica certificata della Direzione Sistemi Informativi e Innovazione dell'ACI.

In caso di mancata tempestiva comunicazione e di conseguente astensione da ogni atto, il Responsabile operativo è ritenuto responsabile per i danni arrecati all'ACI successivamente all'evento che determina la decadenza.

In ogni caso di decadenza del Responsabile operativo, l'ACI può chiedere, a propria discrezione, che venga nominato un nuovo Responsabile operativo oppure procedere direttamente alla abilitazione e disabilitazione delle utenze degli Operatori per la medesima organizzazione.

Il Responsabile operativo rilascia le utenze previa verifica dei requisiti previsti dal Regolamento e procede alla disabilitazione degli Operatori non più in servizio o per i quali non sia più utile l'utenza.

Il Responsabile operativo rilascia l'utenza dopo avere accertato, sotto la propria responsabilità, l'identità dell'Operatore.

L'ACI si riserva di inviare periodicamente l'elenco degli utenti abilitati che il Responsabile operativo è tenuto a verificare allo scopo di disabilitare le utenze non più utilizzate.

In qualunque caso di cessazione del rapporto di servizio dell'Operatore o in ogni caso in cui sia sopravvenuta almeno una delle condizioni indicate al precedente 18, il Responsabile operativo è tenuto in ogni caso a disabilitare immediatamente la relativa utenza.

Nell'esercizio delle funzioni quale Responsabile operativo è tenuto a dare integrale applicazione alle disposizioni normative vigenti in materia di protezione dei dati personali.

L'ACI si riserva la possibilità di effettuare controlli e verifiche sulle Utenze rilasciate dal Responsabile operativo, anche mediante visite presso la sede dell'Organizzazione presso cui è costituito il Responsabile operativo, allo scopo di accertare la regolarità delle utenze rilasciate.

In ogni caso in cui l'ACI venga a conoscenza di irregolarità nel rilascio delle Utenze può, a proprio insindacabile giudizio, assumere i seguenti rimedi, commisurati al livello di gravità della irregolarità rilevata:

- disabilitare l'utenza per la quale sono state rilevate irregolarità, da un minimo di tre mesi oppure permanentemente;
- sospendere il Responsabile operativo per un periodo minimo di tre mesi;
- disporre la decadenza definitiva del Responsabile operativo.

In caso di sospensione del Responsabile operativo, l'ACI può procedere direttamente al rilascio, abilitazione e disabilitazione delle utenze su richiesta del rappresentante legale o Dirigente per l'organizzazione di appartenenza.

In caso di decadenza del Responsabile operativo, l'ACI può, a proprio insindacabile giudizio, procede direttamente a rilasciare, abilitare, disabilitare le utenze per l'organizzazione di appartenenza oppure concedere al rappresentante legale o al Dirigente della medesima organizzazione di nominare un nuovo Responsabile operativo.

L'ACI si riserva in ogni caso di procedere alla denuncia alle autorità competenti in tutti i casi in cui ravvisi nelle irregolarità riscontrate eventuali fatti aventi rilevanza penale

7.5.2 Responsabilità degli utenti

7.5.2.1. Utilizzo delle informazioni segrete di autenticazione

Gli utenti devono essere tenuti a seguire le prassi dell'Ente nell'uso di informazioni segrete di autenticazione, nello specifico:

1. conservare la password con diligenza e nella massima riservatezza, assicurandosi che non sia divulgata ad altri soggetti, incluse figure di autorità; Non scrivere mai la password su post it o foglietti attaccati al computer;
2. evitare di mantenere un registro (ad esempio su carta) di credenziali segrete, a meno che questo non possa essere conservato in modo sicuro e il metodo di memorizzazione sia stato approvato dalla Direzione Sistemi Informativi e Innovazione;
3. provvedere all'immediato cambio delle credenziali segrete in caso di perdita di segretezza o sospetto di compromissione, compresi i casi di smarrimento o furto della dotazione informatica;

4. compatibilmente con i vincoli tecnologici dell'applicazione / servizio, selezionare solo password di almeno 8 caratteri che rispondano ai seguenti requisiti di robustezza:
    a. la password contiene almeno una lettera maiuscola (e.g. A, B, C);
    b. la password contiene almeno una lettera minuscola (e.g. a, b, c);
    c. la password contiene almeno un numero (e.g. 1, 2, 3);
    d. la password contiene caratteri non alfanumerici (e.g. #, &, !, %, @, ?, -, *);
    e. la password non contiene l'utenza, il nome o cognome dell'utente o parole contenute in un dizionario;
    f. la password non contiene ripetizioni di caratteri;
5. modificare sempre al primo accesso le informazioni segrete di autenticazione temporanee ricevute, anche quando l'applicazione/servizio non obbliga a farlo;
6. non utilizzare le stesse credenziali di accesso per scopi aziendali e personali.

7.5.3. Controllo degli accessi ai sistemi e alle applicazioni

7.5.3.1. Limitazione dell'accesso alle informazioni

Al fine di supportare le politiche di controllo degli accessi di ACI, tutte le applicazioni e i servizi in esercizio devono essere configurati, ove possibile, per adottare funzionalità che permettano di controllare i privilegi di accesso degli utenti, quali:

1. controllare quali dati e informazioni possono essere consultati da un particolare utente;
2. controllare i privilegi di accesso degli utenti, ad esempio lettura, scrittura, esecuzione e cancellazione;
3. controllare i privilegi di accesso di altre applicazioni IT;
4. limitare le informazioni contenute negli output a quelle strettamente necessarie.

7.5.3.2. Procedure di log-on sicure

Sistemi e applicazioni devono essere configurati, ove possibile, al fine di adottare procedure di log-on sicure finalizzate a ridurre il rischio di accesso non autorizzato, seguendo le seguenti buone pratiche:

1. non mostrare identificatori di sistemi/applicazioni sino a quando il processo di log-on non sia stato completato con successo;
2. mostrare un avviso generale che avverta che il sistema/applicazione può essere acceduto solo da utenti autorizzati;
3. non fornire messaggi di aiuto durante la procedura di log-on che potrebbero facilitare l'accesso ai sistemi/applicazioni da parte di soggetti non autorizzati;
4. validare le informazioni di log-on solo al termine dell'inserimento di tutti i dati in input. In caso di errore, il sistema non deve indicare quale parte dei dati inseriti sia corretta/errata;
5. proteggere da tentativi di attacco brute-force (o forza bruta), consentendo un numero massimo di 5 tentativi di accesso falliti prima del blocco dell'utenza;

6. registrare tentativi di accesso sia riusciti sia falliti;
7. non mostrare le password mentre vengono digitate;
8. non trasmettere le password in chiaro sulla rete;
9. visualizzare le seguenti informazioni al completamento di un log-on riuscito:
    a. data e ora del precedente log-on riuscito;
    b. dettagli di eventuali tentativi di accesso falliti;
10. ove appropriato, terminare le sessioni inattive dopo 30 minuti di assenza di input da parte dell'utente.

7.5.3.3. Sistema di gestione delle password

I sistemi di gestione delle password devono essere configurati, ove possibile, al fine di assicurare password di qualità, e nello specifico:

1. consentire agli utenti di modificare le proprie password e includere una procedura di conferma per evitare eventuali errori di digitazione;
2. consentire agli utenti di selezionare solo password di qualità, che soddisfino i requisiti identificati nel comma iv del paragrafo 2.3.4;
3. imporre agli utenti la modifica delle password temporanee al primo accesso;
4. imporre modifiche periodiche della password almeno ogni 90 giorni;
5. conservare uno storico delle password utilizzate in precedenza da ciascun utente e impedire il riutilizzo delle ultime 10 password;
6. memorizzare le password separatamente dai dati del sistema applicativo;
7. memorizzare e trasmettere le password in forma cifrata.
8. memorizzare le password in un archivio cifrato a cui può accedere solamente il personale autorizzato. L'accesso a tale archivio deve essere tracciato come log.

Il primo invio delle credenziali può essere effettuato verso un indirizzo mail personale. In tal caso la procedura deve tuttavia prevedere il cambio password automatico al primo accesso.

7.5.3.4. Uso di programmi di utilità privilegiati

Per programmi di utilità privilegiati si intendono tutti quei programmi che, per funzionare correttamente, necessitano di utilizzare utenze con privilegi amministrativi o, in generale, possono essere in grado di aggirare i controlli applicativi e di sistema.

L'uso di tali programmi deve essere limitato e strettamente controllato, e nello specifico:

1. l'utilizzo di tali programmi deve essere limitato nel tempo e previamente concordato e approvato dalla Direzione Sistemi Informativi e Innovazione;
2. l'utilizzo di tali programmi deve essere consentito al solo personale autorizzato per l'esecuzione di attività amministrative sui sistemi o attività richieste dal business;
3. l'utilizzo di tali programmi deve essere loggato, al fine di consentire, ove necessario, un riesame delle attività eseguite;

4. una lista di tali programmi in uso nell'Ente deve essere mantenuta e riesaminata con cadenza almeno annuale, procedendo alla rimozione o disattivazione di tutti i programmi di utilità non più necessari.

7.5.3.5. Controllo degli accessi al codice sorgente dei programmi

È necessario che gli accessi al codice sorgente dei programmi e alle informazioni correlate (e.g. schemi applicativi, specifiche tecniche, piani di test, ecc.), siano limitati. In particolare:

1. ove possibile, il codice sorgente non compilato e informazioni correlate non devono risiedere sui sistemi di esercizio;
2. gli accessi al codice sorgente devono essere limitati al solo personale autorizzato sulla base delle proprie mansioni operative;
3. gli accessi al codice sorgente devono essere loggati;
4. la manutenzione e la copia del codice sorgente deve essere soggetta a rigorose procedure di controllo sulle modifiche.

7.6 Gestione delle eccezioni

Tutte le eccezioni all'applicazione della presente politica devono essere preventivamente concordate con la Direzione Sistemi Informativi e Innovazione, affinché la stessa possa valutare il rischio di sicurezza delle informazioni associato e identificare eventuali opportuni controlli compensativi.

8. Politica di sicurezza per la gestione degli asset informatici in dotazione ai dipendenti

8.1. Scopo e campo di applicazione

Il progressivo sviluppo tecnologico e la rapida diffusione di strumentazioni informatiche dotate di funzionalità sempre più complesse espongono le organizzazioni a problematiche inerenti la sicurezza dei propri asset e del proprio patrimonio informativo.

A tal proposito, è necessario che le organizzazioni si dotino di un processo che disciplini la gestione e l'utilizzo delle dotazioni informatiche messe a disposizione dei propri dipendenti al fine di garantire un adeguato livello di disponibilità, integrità e riservatezza dei dati e delle informazioni aziendali che sono conservate nelle suddette dotazioni.

Scopo del presente documento è pertanto quello di fornire i principi generali e le linee guida in materia di Information Security relative all'assegnazione, alla gestione e all'utilizzo delle dotazioni informatiche messe a disposizione di tutti i dipendenti dell'Automobile Club d'Italia onde ridurre al minimo i rischi di indisponibilità, accesso non autorizzato, distruzione o perdita anche accidentale delle stesse.

È opportuno precisare che l'argomento viene trattato unicamente ai fini della definizione delle Politiche di sicurezza:, non vengono pertanto disciplinati ulteriori aspetti, come quelli amministrativi, contabili e fiscali, che afferiscono alla gestione degli asset informatici.

In particolare, la presente politica ha fra i principali obiettivi di assicurare che:

- i dipendenti dispongano di chiare linee guida circa il corretto utilizzo dei dispositivi aziendali;
- gli asset informatici siano gestiti per l'intera durata del loro ciclo di vita, dall'assegnazione fino alla revoca/dismissione, in conformità alle best practice in materia di Information Security ed in compliance a leggi e regolamenti vigenti;
- i dati trattati mediante dotazioni informatiche siano sicuri e protetti da accessi non autorizzati;
- i dati all'interno degli asset in uso in ACI siano correttamente e opportunamente cancellati prima della dismissione o riassegnazione del dispositivo che li contiene.

Le seguenti linee guida si applicano a tutti i componenti della dotazione informatica messa a disposizione del personale e a tutti i dipendenti ACI. Il mancato rispetto o la violazione delle regole in esso indicate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari, nonché con le azioni civili e penali previste.

Tale policy è inoltre rivolta a tutti i collaboratori esterni (es. consulenti) che, nello svolgimento della propria attività lavorativa, accedono e utilizzano le risorse informative di ACI.

Rimane in ogni caso inteso che:

- per le risorse informative messe a disposizione o date in uso a ACI da altri Enti od organizzazioni valgono gli accordi e le condizioni contrattuali stipulate fra le parti;

- per l'utilizzo di documenti, banche dati, programmi e materiali valgono le condizioni di tutela del diritto d'autore (Copyright), ove previsto;
- le modalità di utilizzo delle risorse informative devono essere sempre conformi a quanto previsto dalle normative nazionali vigenti.

8.2. Normative di riferimento

La presente policy recepisce le best practice e gli standard internazionali applicabili al contesto ed in particolare:

- ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information security management systems requirements;
- ISO/IEC 27002:2013 – Information Technology – Security Techniques – Code of practice for information security controls;
- Circolare AgID n. 1/2017 del 17 marzo 2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Regolamento (UE) 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GDPR);
- D. Lgs. 196/2003 (Codice Privacy) e s.m.i.

8.3. Principali ruoli e responsabilità

Le attività di gestione degli asset informatici prevedono il coinvolgimento di molteplici attori, attivati nelle modalità e nelle tempistiche più opportune, tra cui i principali risultano essere:

- Servizio Patrimonio
- Direzione Risorse Umane e Organizzazione;
- Direzione Sistemi Informativi e Innovazione;
- ACI Informatica;
- Assegnatario.

Per ciascuno di essi, nel presente capitolo vengono descritti i principali compiti e responsabilità in materia di Information Security in ambito alla gestione del ciclo di vita degli asset in dotazione ai dipendenti.

8.3.1. Servizio Patrimonio

In accordo con la Direzione dei Sistemi Informativi e Innovazione, gestisce l'inventario e il ciclo di vita di tutte le risorse informatiche dell'Ente attraverso le procedure SAP.

8.3.2. Direzione Risorse Umane e Organizzazione

La Direzione Risorse Umane e Organizzazione ha la responsabilità di:

1. notificare tempestivamente alla Direzione Sistemi Informativi e Innovazione qualunque evento che comporti una nuova assunzione/assegnazione ad altra struttura o interruzione del rapporto di lavoro a vario titolo, evidenziando la perdita o l'acquisizione di determinate qualità al fine di poter essere dotati di specifici strumenti;
2. identificare e definire, in cooperazione con la Direzione Sistemi Informativi e Innovazione, il set di dotazioni informatiche che ciascun dipendente deve ricevere in assegnazione per assolvere alle proprie mansioni lavorative, sulla base del ruolo ricoperto all'interno di ACI o esigenze lavorative particolari (e.g. telelavoro, smartworking);
3. comunicare la presente politica di sicurezza ai nuovi assunti, nonché le regole per il corretto utilizzo degli strumenti aziendali contenute nel disciplinare tecnico allegato alle "Politiche di Sicurezza dei Sistemi e delle Informazioni" di ACI.

8.3.3. Direzione Sistemi Informativi e Innovazione

La Direzione Sistemi Informativi e Innovazione è responsabile per:

1. la consegna dell'hw e l'assegnazione in SAP del cespite relativo a postazioni fisse;
2. la consegna dell'hw mobile, l'assegnazione in SAP e la redazione del verbale di assegnazione protocollato e controfirmato dall'assegnatario;
3. garantire l'identificabilità e la tracciabilità degli asset informatici in dotazione ai dipendenti ACI attraverso la redazione e il costante aggiornamento di un appropriato Asset Inventory dell'hw.

È inoltre responsabile per:

4. la definizione delle principali policy di sicurezza relativamente alle dotazioni informatiche, inclusi laptop, PC fissi e dispositivi mobili;
5. definire, perfezionare e mantenere le regole di sicurezza da applicare nel processo di gestione degli asset informatici, al fine di garantire che ACI sia conforme a tutta la normativa cogente ed ai regolamenti interni che riguardano la sicurezza e l'integrità dei dati, detenuti sui dispositivi di proprietà di ACI ed utilizzati dagli assegnatari.

8.3.4 ACI Informatica

ACI Informatica è responsabile per:

la configurazione, consegna, installazione, manutenzione e dismissione sicura delle dotazioni informatiche in coerenza con quanto stabilito dal presente documento e dalle altre politiche di sicurezza aziendali;

l'installazione, l'aggiornamento, il monitoraggio ed il corretto funzionamento dei presidi tecnologici di sicurezza previsti sui suddetti dispositivi e finalizzati a mitigare il rischio di sicurezza delle informazioni.

identificare i presidi tecnologici minimi che devono essere implementati sulle diverse tipologie di asset informatici al fine di ridurre il rischio di sicurezza delle informazioni ad un livello accettabile, non potendo generalmente ottenere l'annullamento integrale dello stesso;

verificare la corretta applicazione della presente politica.

8.3.6. Assegnatario

Gli assegnatari sono responsabili del corretto e consapevole utilizzo delle dotazioni informatiche e delle abilitazioni affidategli da ACI, anche qualora essi non coincidano con i reali utilizzatori delle stesse, come ad esempio nel caso di dotazioni utilizzate da consulenti esterni o assegnate a Uffici Periferici. In quest'ultimo caso, infatti, le dotazioni potrebbero essere assegnate al Responsabile dell'Ufficio e messe a disposizione di tutte le risorse appartenenti all'Ufficio stesso, attraverso l'utilizzo di account di dominio strettamente personali.

Tutti gli assegnatari, indipendentemente se collaboratori esterni o dipendenti appartenenti ad Uffici Periferici/sedi centrali di ACI, sono tenuti ad adottare tutte le precauzioni a tutela del corretto funzionamento delle dotazioni assegnategli e della sicurezza delle informazioni aziendali/personali accessibili o elaborate per loro tramite, applicando quanto previsto dal presente documento e dalle altre politiche aziendali per la sicurezza.

Il dipendente è tenuto ad assicurare la protezione e la conservazione dei beni informatici dell'Amministrazione, materiali e immateriali, avuti in affidamento per l'espletamento dei propri compiti, ed è responsabile del relativo utilizzo in modo improprio e non conforme ai fini istituzionali. In caso di inefficienza, guasto o deterioramento delle risorse materiali e strumentali affidate, ne dà immediata comunicazione al dirigente o al responsabile della struttura di appartenenza[7].

Al dipendente è consentito utilizzare gli strumenti informatici messi a disposizione dall'Amministrazione per poter assolvere alle incombenze personali, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

Al dipendente - ai fini dell'erogazione delle prestazioni di lavoro, con particolare riferimento alla modalità agile - è consentito l'utilizzo di dispositivi elettronici personali assicurando il rispetto delle condizioni di sicurezza nell'utilizzo[8].

8.4. Tipologia di asset informatici forniti dall'Ente

[7] V. Codice di comportamento, art. 13
[8] V. Codice di comportamento, ar. 16

Gli asset informatici in dotazione ai dipendenti di ACI sono contraddistinti da un elevato grado di eterogeneità in termini di tipologia di dispositivi utilizzati e caratteristiche tecnologiche specifiche dei singoli dispositivi.

In generale, essi possono essere fatti afferire alle seguenti macro-categorie:

Postazioni di Lavoro (PdL) fisse, intese come il complesso costituito da componenti hardware (e.g. Personal Computer Desktop) e software (Sistema Operativo, Antivirus, Suite Openoffice, Google Apps, ecc.) attraverso il quale i dipendenti rendono la propria prestazione lavorativa.

Tali postazioni si contraddistinguono dalle altre tipologie di dotazioni contenute nella presente lista perché sono utilizzate esclusivamente all'interno degli edifici di ACI e sfruttano le sole connessioni aziendali. Per questo motivo, esse sono esposte ad un rischio inerente di Information Security inferiore a quello di dotazioni rimovibili, che per propria natura sono esposte a rischi di furto, smarrimento, ecc.

Una importante distinzione che deve essere operata in tale ambito è quella tra le PdL utilizzate nelle sedi strutture centrali di ACI, che sono assegnate in maniera diretta a ciascuno specifico dipendente e le PdL dislocate presso gli Uffici delle Sedi Provinciali, che sono invece assegnate al Responsabile dell'Ufficio e messe a disposizione di tutte le risorse appartenenti all'Ufficio interessato, attraverso l'utilizzo di account di dominio strettamente personali.

Postazioni di lavoro mobili (Laptop). Tali dispositivi sono assimilabili per funzionalità e tecnologia alle Postazioni di Lavoro fisse ma si contraddistinguono per essere predisposti al trasporto a mano da parte di una sola persona.

A causa della propria natura, la postazione di lavoro mobile richiede l'adozione di particolari cautele, dettate dal buon senso e dalle specifiche situazioni, atte a prevenirne il furto e garantire la protezione delle informazioni in essa contenute. Tali dispositivi richiedono pertanto l'implementazione di controlli di sicurezza specifici rispetto alle Postazioni di Lavoro fisse, dedicati a mitigare tali rischi aggiuntivi.

Dispositivi mobili (e.g. tablet e smartphone). Tali dispositivi sono caratterizzati da dimensioni ridotte, almeno un'interfaccia di rete wireless, possibilità di utilizzare carte SIM per usufruire di servizi voce e dati, memorizzazione locale dei dati, download delle applicazioni diversificato (e.g. acquistate tramite web browser o Application Store incorporato nel dispositivo) e sistemi operativi diversi da quelli delle PdL e Laptop.

Tali dispositivi sono assegnati ad un sottoinsieme ristretto di dipendenti ACI, sulla base dello specifico ruolo ricoperto all'interno di ACI o di specifiche esigenze lavorative o di mobilità.

Essi comportano tutti i rischi aggiuntivi che caratterizzano i dispositivi Laptop a causa della loro portabilità e presentano difficoltà di gestione aggiuntive, causate dell'utilizzo di tecnologie e paradigmi non assimilabili ai suddetti. Tali dotazioni richiedono, pertanto, la definizione di politiche e presidi tecnologici dedicati e finalizzati a mitigare i rischi che esse introducono in ACI.

È vietata qualsiasi attività che possa produrre danni, diretti o indiretti, alle risorse informative o accessi non autorizzati alle informazioni in esse contenute e che risulti in contrasto con le regole contenute nel presente testo, con le normative emanate da ACI o con la legislazione vigente.

8.5. Politiche di sicurezza

Nel presente paragrafo sono descritte le politiche di sicurezza che ACI ha definito per la protezione delle proprie risorse informative assegnate al personale aziendale, sia di carattere generale, sia per specifica tipologia di asset.

8.5.1 Regole generali

Tutte le postazioni sono configurate secondo uno standard approvato dalla Direzione Sistemi Informativi e Innovazione. La richiesta di installazione su postazioni di singoli Dipendenti di programmi software non compresi nella dotazione standard deve essere preventivamente approvata dal Direttore delle Struttura di appartenenza del Dipendente ed inoltrata alla Direzione Sistemi Informativi e Innovazione. Quest'ultima autorizza l'installazione del software richiesto previa verifica della compatibilità con la restante dotazione e dell'assenza di qualunque rischio per la sicurezza.

Devono essere sviluppati standard di configurazione per tutte le tipologie di asset informativi, ove applicabile. È necessario accertarsi che tali standard mitighino tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di hardening accettati come best practice di settore.

I parametri di sicurezza delle dotazioni, ove possibile, devono essere configurati per evitarne un uso improprio.

Tutte le funzionalità non necessarie che potrebbero introdurre rischi di sicurezza devono essere rimosse/disabilitate dalle dotazioni prima che le stesse vengano consegnate agli assegnatari.

È necessario modificare sempre i valori predefiniti del fornitore e rimuovere o disabilitare account predefiniti non necessari prima di fornire le dotazioni ai dipendenti. Questo vale per tutte le password predefinite, incluse, senza limitazioni, quelle utilizzate da sistemi operativi, software che fornisce servizi di sicurezza, account di applicazioni e sistemi, ecc.

8.5.1.1 Utilizzo ed accesso agli asset aziendali

1. L'accesso alle dotazioni informatiche deve essere, ove applicabile, autenticato.
2. Tutti gli utenti hanno diritto ad accedere alle sole risorse informatiche aziendali per le quali sono stati espressamente autorizzati e ad utilizzarle esclusivamente per l'espletamento della propria operatività quotidiana.

3. L'accesso a utenze e funzionalità privilegiate delle dotazioni informatiche deve essere limitato alla quantità minima necessaria a ciascun dipendente per lo svolgimento delle proprie mansioni lavorative e sulla base del ruolo ricoperto all'interno di ACI.
4. Tutti gli utenti sono tenuti ad adottare, nell'ambito delle proprie attività quotidiane tutte le misure di sicurezza e di buon senso atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche (ad es. non lasciarle incustodite, non concederle in comodato d'uso, seppure gratuito, non venderle, ecc.). Ciascun soggetto è tenuto ad uniformarsi alle suddette prescrizioni ed a segnalare eventuali violazioni alle medesime alla Direzione Sistemi Informativi e Innovazione.
5. È necessario garantire la formazione del personale, che deve essere a conoscenza delle buone pratiche di sicurezza, regole per la custodia ed il corretto utilizzo dei dispositivi in dotazione.
6. Ciascun utente è tenuto a sottoporre periodicamente a backup tutte le informazioni memorizzate sulle risorse aziendali assegnategli.

8.5.1.2 Segnalazione di eventi

Lo smarrimento, la sottrazione, la manomissione, l'accesso non autorizzato o il danneggiamento di una dotazione informatica aziendale deve essere segnalato tempestivamente in conformità alla policy di Incident Management e alle relative procedure.

In caso di rilevazione di particolari anomalie, guasti o malfunzionamenti, l'utente è invitato a comunicarlo tempestivamente, in conformità alla policy di Incident Management e alle relative procedure.

Se l'utente ritiene che il proprio pc è infettato da un malware deve:

- scollegarlo subito dalla rete
- segnalare al Presidio tecnico di Aci Informatica e al Referente Territoriale DSII per procedere alla "pulizia" del computer e nel dubbio formattarlo e per l'eventuale controllo di ogni altro computer nella rete.

8.5.1.3 Configurazione degli asset

Per il corretto funzionamento delle applicazioni e per evitare compromissioni (e.g. accessi abusivi, virus informatici, trattamento illecito, ecc.) sia alle apparecchiature sia all'interno della rete di ACI, è opportuno che l'utente:

- non modifichi, senza preventiva autorizzazione, le configurazioni hardware e software impostate sulle dotazioni informatiche affidate in uso;
- non rimuova o modifichi, senza preventiva autorizzazione, le applicazioni o le dotazioni aziendali;

- non installi sulle dotazioni informatiche, senza preventiva autorizzazione, mezzi di comunicazione o altre periferiche proprie (e.g. modem, masterizzatori, ecc.);
- non installi ed utilizzi software/applicazioni non autorizzate da ACI, sebbene legali (ad es. programmi salvaschermo, software peer-to-peer, software/applicazioni gratuite e liberamente scaricabili da internet c.d. freeware). Qualora siano installati programmi non autorizzati, questi potranno essere disinstallati dal personale tecnico addetto alla manutenzione (anche senza preavviso);
- non utilizzi software ricevuto in uso al di fuori delle finalità lavorative evitando, in particolare, di realizzare copie da cedere, a qualsiasi titolo, a terzi;
- non utilizzi e/o distribuisca (anche via e-mail) software che possa danneggiare le dotazioni informatiche;
- o non utilizzi sul proprio computer né file multimediali (e.g. .MP3, .AVI, .MP4, .MPEG, ecc.) né eBook, norme, documentazione ecc. ottenuti in violazione della normativa sul diritto d'autore;
- non apra file allegati a messaggi di posta elettronica di provenienza non sicura;
- non installi apparecchiature atte ad intercettare o impedire le comunicazioni relative ad un sistema informativo o ad effettuare accessi non autorizzati;
- non introduca volontariamente un codice malevolo nei sistemi informativi (e.g. virus, worm, trojan horse, ecc.).

8.5.1.4 Identificazione e gestione degli asset

Tutti gli asset informatici messi a disposizione degli assegnatari devono essere chiaramente identificati e tracciati all'interno di un apposito inventario (vedi capitolo "Asset Inventory").

L'inventario degli asset deve essere accurato, aggiornato, coerente e allineato con altri inventari. Per ciascun asset identificato, deve essere chiaramente identificato un owner (vedi capitolo "Asset Inventory").

Deve essere definito un formale processo per la gestione sicura dell'intero ciclo di vita degli asset, dall'assegnazione fino alla revoca/dismissione, in conformità alle best practice in materia di Information Security ed in compliance a leggi e regolamenti vigenti (vedi capitolo "Processo di gestione delle dotazioni informatiche").

8.5.1.5 Meccanismi di protezione

Il software antivirus deve essere distribuito su tutti i sistemi solitamente interessati da malware, ove applicabile. Ogni utente è, altresì, tenuto a:

- controllare la presenza ed il regolare funzionamento del software antivirus installato;
- segnalare prontamente alla Funzione competente il caso in cui il software antivirus non riesca automaticamente ad eliminare la minaccia dai sistemi aziendali;
- verificare con il software antivirus, prima dell'apertura di qualsiasi file, ogni dispositivo (e.g. pen-drive, hard disk esterni, ecc.) proveniente dall'esterno e il cui utilizzo sia stato preventivamente autorizzato.

È necessario verificare che tutti i meccanismi antivirus siano aggiornati periodicamente e configurati per eseguire scansioni periodiche e non possano essere disattivati o modificati dagli utenti.

Tutte le dotazioni informative in utilizzo ai dipendenti devono essere protette dalle vulnerabilità note mediante l'installazione delle patch di sicurezza dei fornitori, installando almeno le patch di sicurezza critiche entro un mese dalla release.

All'interno delle dotazioni informatiche, in particolare quelle mobili, non devono essere memorizzate informazioni aziendali sensibili o di business se non è possibile applicare una protezione adeguata al loro livello di classificazione.

È altamente raccomandato di non utilizzare pen-drive per il trasferimento dei dati. La modalità normale per trasferire documenti e file è costituita dalla posta elettronica e Drive. Quest'ultimo può essere utilizzato anche per il trasferimento di file di grandi dimensioni ed anche verso utenti esterni (anche se non dovessero essere dotati di account Gmail).

Per esigenze di sicurezza è stato bloccato l'accesso a siti utilizzati per il trasferimento di file (es. WeTransfer) in quanto non ritenuti idonei per il rispetto di parametri minimi di sicurezza.

8.5.2 Regole specifiche

Le regole specifiche riguardano le seguenti tipologie di asset.

8.5.2.1 Postazioni di lavoro

Ai fini di un uso accettabile delle postazioni di lavoro fisse è necessario adottare almeno le seguenti regole specifiche.

1. Alle reti aziendali devono essere collegate solo PdL verificate e approvate da ACI.
2. L'uso di PdL individuali, anche temporaneo, da parte di un utente diverso dall'assegnatario, deve essere preventivamente autorizzato.
3. La PdL assegnata deve essere lasciata in condizioni di sicurezza durante un'assenza dal posto di lavoro, seppur di breve periodo (ad es. chiudendo la sessione di lavoro, bloccando la PdL con password, abilitando il blocco a tempo tramite "screen saver" automatico, ecc.), al fine di evitare accessi non autorizzati da parte di terzi.
4. Nel caso in cui sia necessario lasciare la PdL nelle mani di un tecnico, dipendente o di terze parti, per operazioni di manutenzione hw/sw o di sostituzione, può essere concesso l'accesso con le credenziali dell'utente che necessita assistenza a condizione che quest'ultimo mantenga per quanto possibile una vigilanza sulle operazioni compiute sulla propria dotazione informatica.

8.5.2.2 Laptop

Ai laptop e ad altri dispositivi mobili si applicano tutte le regole di utilizzo ed i divieti previsti per le PdL collegate alla rete locale. Il loro uso richiede tuttavia maggiori precauzioni atte a prevenirne il furto/smarrimento e garantire la protezione delle informazioni in funzione del relativo livello di sensibilità.

Ai fini di un uso accettabile dei laptop è necessario adottare almeno le seguenti regole specifiche:

In caso di uso all'interno della Sede aziendale o degli Uffici periferici la miglior protezione contro la sottrazione o smarrimento di un laptop è l'utilizzo sistematico di un apposito cavo di bloccaggio;

In caso di uso esterno o il luoghi pubblici (e.g. alberghi, treni ecc.), l'utente è tenuto ad adottare la massima diligenza nell'utilizzo e conservazione del proprio laptop, con particolare riguardo alla sua custodia (e.g. conservare il laptop nella cassaforte della camera di albergo).

Le informazioni sensibili e di business memorizzate nei laptop devono essere protette da divulgazioni non autorizzate per mezzo di misure appropriate, come meccanismi di crittografia; nel caso in cui non sia possibile applicare misure adeguate, non è consentito mantenere tali informazioni sugli asset informatici.

L'utilizzo di laptop richiede agli assegnatari di collegare frequentemente (orientativamente ogni settimana) la dotazione informatica alla rete aziendale in modo da garantire gli aggiornamenti automatici specifici (e.g. aggiornamento antivirus, patch di sicurezza, ecc.)

Quando collegati a reti diverse da quella aziendale, i laptop devono utilizzare sistemi di crittografia forte (come reti private virtuali VPN) al fine di proteggere la riservatezza e l'integrità delle comunicazioni.

Quando collegati a reti diverse da quella aziendale, i laptop devono utilizzare meccanismi di autenticazione reciproca (e.g. protocollo TLS) per verificare le identità di entrambi gli endpoint prima della trasmissione dati.

È vietato agli utenti l'accesso con il proprio laptop a reti Wi-Fi pubbliche e non protette su siti web non crittografati (ovvero con protocollo HTTP e non HTTPS), le quali non garantiscono la massima sicurezza del dispositivo utilizzato.

8.5.2.3 Dispositivi mobili

Ai fini di un uso accettabile dei dispositivi mobili è necessario adottare almeno le seguenti regole specifiche:

1. Ogni assegnatario di un telefono cellulare ovvero di qualsiasi dispositivo per la telefonia mobile (e.g. tablet), ivi comprese anche le sole schede SIM, ha l'obbligo di utilizzare detti strumenti per l'espletamento della propria operatività quotidiana ed in linea con le motivazioni (e.g. esigenze di reperibilità) che hanno autorizzato la consegna di tale specifica dotazione.

2. L’accesso tramite dispositivi mobili alla rete aziendale ed ai relativi servizi informatici (e.g. connessione di cellulari alla posta aziendale via VPN) è consentito soltanto con strumenti forniti in dotazione da ACI o comunque specificatamente configurati dalla funzione competente.
3. I dispositivi mobili devono essere configurati in modo da richiedere l’autenticazione per l’accesso al dispositivo ed alle risorse dell’organizzazione. Tale configurazione non deve poter essere disabilitata dall’utente.
4. Qualora vengano utilizzati per memorizzare dati sensibili o di business, i dispositivi mobili devono adottare soluzioni di crittografia della memoria locale.
5. È vietato eseguire attività che incidano sull’integrità dei dispositivi forniti da ACI, come operazioni di jailbreaking o rooting.
6. Devono essere previste soluzioni tecnologiche che permettano il wiping remoto del disco in caso di furto o smarrimento del dispositivo mobile.

8.6. Asset Inventory

Come illustrato precedentemente, tutti gli asset informatici messi a disposizione dei dipendenti per l’espletamento della propria prestazione lavorativa devono essere registrati e tracciati in un apposito inventario (Asset Inventory).

Tale inventario deve:

1. essere accuratamente compilato, gestito e manutenuto sulla base di un processo di revisione/aggiornamento condotto su frequenza annuale;
2. utilizzare formati compatibili di censimento;
3. identificare univocamente gli asset al suo interno.

Risulta di fondamentale importanza che i dati in esso contenuti siano esatti e coerenti, garantendo l'esatta corrispondenza tra i dati presenti nell'inventario e la situazione reale rilevabile on-site, in special modo relativamente alla locazione fisica dell’asset, numerazione IP e licenze software installate, dandone pronta comunicazione nel caso di disallineamento.

Di seguito si riportano quelle che sono le principali best practice in materia di Information Security che devono essere adottate per la gestione del sistema di Asset Inventory:

1. Prevedere un unico inventario degli asset a livello di società o, nel caso in cui si ricorra ad un inventario distribuito, garantire comunque univocità nella struttura, nel formato e nei processi di tenuta e gestione.
    a. Identificare ogni asset censito nell’inventario mediante l’assegnazione di:
       Codice d’inventariazione;
       Numero seriale;
    b. Breve descrizione del tipo di dotazione;
    c. Responsabile dell’asset;
    d. Assegnatario dell’asset;
    e. Collocazione dell’asset;
    f. Indirizzo IP, per tutte le risorse collegate alla rete (a cura di ACI Informatica).

2. Prevedere, all'interno del modello di inventario definito, una modalità di classificazione e codifica degli asset che ne garantisca l'identificazione a livello di tipologia (es. PdL, supporto di memoria ecc.).
3. Individuare per ogni asset o classe di asset (e.g. sulla base delle funzioni assolte/servizi erogati e della tipologia di asset) un Responsabile degli stessi per il reperimento delle informazioni richieste all'atto di un eventuale censimento o dell'aggiornamento dell'inventario.
4. Il Responsabile dell'asset deve altresì identificare/approvare i controlli implementati per fornire protezione adeguata all'asset stesso e verificare periodicamente le restrizioni di accesso, tenendo conto delle politiche interne di controllo degli accessi.
5. Comunicare tempestivamente alla struttura aziendale preposta alla tenuta dell'inventario l'eventuale cambiamento di assegnazione di un asset già inventariato, che comporti una variazione dell'ubicazione del bene o dell'assegnatario.
6. Prevedere un processo formalizzato che garantisca l'integrazione dell'inventario ogni qualvolta nuovi asset si aggiungano a quelli già inventariati.
7. Prevedere un processo formalizzato che con una frequenza adeguata verifichi l'attendibilità dei dati presenti nell'inventario per un campione significativo di ogni tipologia censita.
8. Prevedere revisioni periodiche (almeno annuali) circa le tipologie di asset previste da inventariare e le informazioni da censire in inventario per ciascuna tipologia.

8.6.1. Processo di gestione delle dotazioni informatiche

Come illustrato precedentemente, al fine di garantire la riservatezza, integrità e disponibilità del patrimonio informativo di ACI, le dotazioni informatiche devono essere gestite, lungo il loro intero ciclo di vita, secondo un formale processo conforme alle best practice in materia di Information Security ed in compliance a leggi e regolamenti vigenti.

Tale processo deve considerare almeno i seguenti aspetti:

1. Richiesta e autorizzazione nuove dotazioni
2. Configurazione e consegna
3. Rinnovo tecnologico delle dotazioni
4. Cambio di ruolo/mansione lavorativa
5. Restituzione
6. Sostituzione per furto/smarrimento
7. Movimentazioni fisiche
8. Dismissione

8.6.2. Richiesta e autorizzazione nuove dotazioni

La richiesta di nuove dotazioni informatiche può avvenire:

1. dalla Direzione Risorse Umane e Organizzazione al momento dell'ingresso di una nuova risorsa in ACI;

2. dalla Direzione Risorse Umane e Organizzazione in caso di cambio di ruolo/mansione lavorativa di un dipendente;
3. da parte di dipendenti che necessitano di eventuali dotazioni aggiuntive rispetto quelle assegnate di base;
4. da parte di tutte le Direzioni Centrali, Servizi od Uffici di Sede Centrale;
5. da parte di tutti gli Uffici Periferici (PRA) per il tramite del Direttore/RUT;
6. da parte di ACI Informatica per implementazioni/sostituzioni hw.

La richiesta di nuova dotazione si intende implicitamente autorizzata nel processo di assunzione della nuova risorsa. Al contrario, l'eventuale variazione della dotazione informatica a causa di cambio ruolo/mansione o la richiesta di dotazione aggiuntiva da parte del dipendente deve essere preventivamente autorizzata dal Direttore della struttura a cui appartiene il dipendente stesso e opportunamente motivata sulla base di specifiche esigenze legate all'espletamento delle mansioni lavorative o di mobilità.

In tutti i casi sopracitati, e con special riferimento alla gestione di richieste non ordinarie/eccezioni, il processo di gestione delle dotazioni deve essere guidato dal principio della Segregation of Duties (SoD), affinché nessun attore all'interno del processo possa disporre di poteri illimitati e svincolati dalla verifica di altri attori. In particolare, in tale ambito, è opportuno tenere sempre distinte le responsabilità di "chi fa la richiesta" rispetto "chi la autorizza/rigetta".

8.6.3. Configurazione e consegna

Prima dell'effettiva consegna della dotazione informatica al dipendente, questa deve essere configurata sulla base dei principi contenuti nella presente politica e delle procedure operative di dettaglio, cui si fa rimando (vedi capitolo "Politiche di sicurezza").

All'atto della consegna di una nuova dotazione/dotazione aggiuntiva deve essere inoltre predisposto un verbale di assegnazione (solo per specifiche dotazioni quali, laptop, cellulari di servizio, tablet, SIM di servizio) che il dipendente deve sottoscrivere, contenente almeno il set minimo di dati necessario ad identificare univocamente la dotazione informatica ed il relativo assegnatario (nome, cognome, e-mail e telefono).

Deve, infine, essere indicato a ciascun dipendente e in aggiunta a tale policy, il riferimento all'art. 47 del documento "Disciplinare sui sistemi di telefonia e i connessi sistemi di telecomunicazione", che fornisce le linee guida necessarie per la corretta custodia ed utilizzo degli strumenti informatici aziendali e pubblicato sul Portale della Comunicazione Interna, in seguito ad approvazione degli Organi dell'Ente.

8.6.4. Rinnovo tecnologico delle dotazioni

All'interno dei criteri considerati per il rinnovo tecnologico, oltre a criteri di efficienza ed economicità, devono essere opportunamente considerati anche i criteri legati alla sicurezza del parco tecnologico previsto.

In particolare, nel corso delle revisioni periodiche che vengono eseguite sull'Asset Inventory, per tutte le dotazioni informatiche in uso ai dipendenti devono essere valutati fattori come:

- la continua adeguatezza e rispondenza ai criteri di sicurezza di ACI;
- l'eventuale interruzione di supporto da parte del fornitore;
- la continua disponibilità di patch di sicurezza;
- presenza di eventuali vulnerabilità note non sanabili tramite aggiornamenti software.

Per tutti le dotazioni che, secondo i criteri di cui sopra o per ulteriori eventuali motivi, dovessero essere considerate non sicure, è necessario prevedere una sostituzione in tempi ristretti o l'implementazione di opportuni controlli compensativi finalizzati a mitigare il rischio associato.

8.6.5. Cambio di ruolo/mansione lavorativa

Cambi di ruoli e mansioni lavorative del personale ACI devono essere tempestivamente notificati alla funzione competente da parte della Direzione Risorse Umane e Organizzazione, al fine di valutare gli impatti sulle dotazioni informatiche e le abilitazioni assegnate al dipendente coinvolto.

In seguito a tale segnalazione, deve essere implementata un'opportuna procedura che contempli una valutazione di congruenza tra le dotazioni (inclusi pacchetti software e le applicazioni) e le abilitazioni assegnate al dipendente ed il nuovo ruolo ricoperto all'interno di ACI e relative mansioni, prevedendo un opportuno processo di adeguamento, se necessario.

8.6.6. Restituzione

Le dotazioni, complete di tutte le componenti e degli accessori assegnati, devono essere restituite da parte del dipendente nei seguenti casi:

- cessazione del rapporto di lavoro con ACI;
- obsolescenza o esigenza di rinnovo tecnologico della dotazione informatica;
- cambio di ruolo/mansione (vedi paragrafo "Cambio di ruolo/mansione lavorativa"), laddove non sia possibile la conservazione di dotazioni informatiche precedentemente assegnate.

In caso di cessazione del rapporto di lavoro l'utente è tenuto a restituire definitivamente la dotazione informatica assegnatagli.

Inoltre, al fine di tutelare la riservatezza dei dati personali, le funzioni competenti devono provvedere all'eliminazione di tutte le informazioni in essa contenute e disabilitare prontamente tutti gli accessi dell'utente ai sistemi informatici di ACI.

Al momento della restituzione, secondo criteri di economicità ed in una logica di ottimizzazione complessiva degli asset ICT, ACI valuta se riassegnare le dotazioni restituite

o procedere alla loro dismissione. In entrambi i casi devono essere previste misure ed accorgimenti volti a prevenire accessi non consentiti ai dati in essi conservati. Tali misure devono consentire l'effettiva cancellazione delle informazioni o garantire la loro non intelligibilità.

Pertanto, qualunque tipo di supporto di memorizzazione contenente dati personali e qualunque dispositivo contenente informazioni riservate deve essere oggetto di procedure di cancellazione sicura.

Nel caso in cui la dotazione informatica sia destinata a reimpiego e, dunque, riassegnazione ad altro utente, l'effettiva cancellazione dei dati può essere ottenuta, a titolo esemplificativo, con:

- utilizzo di software quali wiping program o file shredder;
- formattazione completa dei dispositivi di tipo hard-disk.

Per la dotazione informatica destinata a smaltimento, invece, si faccia riferimento al successivo paragrafo "Dismissione".

Al momento della restituzione, deve essere data la possibilità al dipendente che ne faccia esplicita richiesta, di salvare i soli dati personali.

In caso di restituzione per obsolescenza/esigenza di sostituzione, deve essere previsto un processo di migrazione dei dati dalla vecchia alla nuova dotazione, prima di procedere alla distruzione degli stessi sull'apparato in dismissione/sostituzione.

Infine, ogni evento correlato a restituzione di asset informatici deve essere prontamente recepito e tracciato all'interno dell'Asset Inventory (vedi capitolo "Asset Inventory").

8.6.7. Sostituzione per furto o smarrimento

In caso di furto o smarrimento delle apparecchiature informatiche deve essere prevista una procedura che contenga almeno i seguenti passi:

1. presentazione di una denuncia da parte dell'Assegnatario alle locali Autorità di Polizia, completa di tutti i relativi dati di identificazione dell'asset smarrito (codice IMEI, marca, modello, data di smarrimento ecc.);
2. tempestiva comunicazione della denuncia (via mail) alle funzioni competenti ACI;
3. reset password relativamente all'account di dominio ed all'account di posta elettronica interessato;

in caso di smarrimento o furto di un tablet o di un dispositivo mobile, blocco immediato del dispositivo stesso (codice IMEI) e della relativa SIM.

L'eventuale diffusione non autorizzata delle informazioni contenute nei dispositivi oggetto di furto o smarrimento, oltre a danneggiare ACI, può esporlo, in qualità di Titolare del trattamento di dati personali, alle sanzioni previste nella normativa privacy vigente.

8.6.8. Movimentazioni fisiche

È necessario che gli asset e i supporti che contengono le informazioni siano protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto. A tale scopo, devono essere considerate le seguenti linee guida:

1. il servizio di movimentazione degli asset informatici di proprietà di ACI è affidato esclusivamente a corrieri espressi selezionati tramite procedura di gara pubblica;
2. devono essere sviluppate e applicate procedure di identificazione dei corrieri;
3. deve essere tenuta traccia scritta di tutti i trasferimenti, che identifichi puntualmente gli asset trasferiti, le cautele adottate, date, orari e persone coinvolte nei cambi di custodia, e traccia della ricezione finale.

8.6.9. Dismissione

Indipendentemente dalle cause scatenanti (e.g. obsolescenza, danneggiamento, ecc.), la dismissione dei dispositivi non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali. Tali procedure devono considerare almeno:

1. la cancellazione sicura o distruzione fisica (e.g. punzonatura, deformazione meccanica, degaussing) delle memorie contenute negli asset informatici in dismissione.
2. il mantenimento di una traccia di audit (audit trail) afferente alle attività di dismissione.
3. il tempestivo aggiornamento dell'*Asset Inventory*.

Anche qualora il servizio di smaltimento/dismissione venga affidato a soggetti terzi, la cancellazione sicura dei dati contenuti nei dispositivi da smaltire deve essere effettuata da parte di ACI, antecedentemente alla consegna dei suddetti dispositivi ai fornitori incaricati.

Ogni apparecchiatura HW dotata di hard disk deve essere affidata per lo smaltimento a ditte specializzate in grado di poter rilasciare la certificazione dell'avvenuta distruzione dell'hard disk.

In alternativa allo smaltimento e nel rispetto di quanto previsto dal manuale delle procedure negoziali, i computer (qualora siano in condizione di potere essere riutilizzati) possono essere donati ad Enti e Organizzazioni no profit. In tal caso il Dirigente o il Responsabile della Struttura che cura la donazione deve assicurare che l'hard disk sia stato formattato allo scopo di eliminare il rischio della fuoriuscita di dati personali precedentemente memorizzati.

9. Politica per la gestione degli incidenti di sicurezza delle informazioni

9.1. Scopo

Politiche e controlli di sicurezza delle informazioni non possono garantire la totale protezione delle informazioni, dei sistemi informativi, dei sistemi e delle reti di ACI. In seguito all'implementazione dei controlli, è infatti probabile che nell'ambito del Sistema di Gestione della Sicurezza Informatica permangano vulnerabilità residue che ne possano minare l'efficacia. Tali vulnerabilità, se sfruttate, potrebbero generare impatti avversi, sia di tipo diretto sia indiretto, sulla continuità delle operazioni dell'Ente.

Inoltre, è inevitabile che nell'ambito della continua progressione tecnologica, che conduce all'introduzione di nuovi strumenti a supporto dell'operatività quotidiana nonché all'evoluzione di quelli esistenti, nuove minacce precedentemente non identificate possano manifestarsi e causare incidenti di sicurezza delle informazioni. Una preparazione insufficiente da parte di ACI nella gestione di questi incidenti potrebbe inficiare l'efficacia delle azioni di risposta, nonché incrementare i potenziali impatti avversi sulle operazioni.

Scopo del presente documento è pertanto quello di descrivere le politiche adottate da ACI per consentire un approccio strutturato e sistematico alla gestione degli incidenti di sicurezza delle informazioni. Tali politiche devono essere recepite da ACI nonché dal proprio partner tecnologico, ACI Informatica, in qualità di Responsabile esterno del trattamento informatizzato dei dati di titolarità di ACI, al fine di garantire che:

- gli eventi di sicurezza siano rilevati e gestiti in maniera efficace ed efficiente, identificando in particolare qualora essi debbano essere categorizzati e classificati come incidenti oppure no;
- gli incidenti di sicurezza identificati vengano valutati, analizzati e affrontati nella maniera più appropriata ed efficiente;
- gli effetti avversi degli incidenti di sicurezza sull'operatività di sistemi e utenti impattati siano minimizzati come parte della risposta all'incidente, eventualmente anche tramite l'attivazione di piani per la gestione delle crisi;
- le vulnerabilità del sistema di gestione della sicurezza delle informazioni vengano valutate e affrontate tempestivamente e appropriatamente;
- la gestione di vulnerabilità e incidenti di sicurezza produca lesson learnt, che possano essere utilizzate per prevenire futuri incidenti di sicurezza, migliorare l'implementazione dei controlli di sicurezza e affinare il processo di gestione degli incidenti di sicurezza delle informazioni.

A tale scopo, le politiche descritte all'interno del presente documento sono allineate agli standard e le *best practice* internazionali di settore.

9.2. Campo di applicazione

Le politiche contenute all'interno del presente documento si applicano a tutti gli eventi e agli incidenti di sicurezza delle informazioni che possono impattare la sicurezza del patrimonio informativo di ACI, in termini di perdita di riservatezza, disponibilità e integrità dello stesso.

Le regole della presente procedura si applicano al personale di ACI, del suo partner tecnologico ACI Informatica, in qualità di Responsabile esterno del trattamento informatizzato dei dati di titolarità di ACI, nonché di tutte le terze parti che intrattengono rapporti di qualunque natura con le suddette (consulenti, personale temporaneo, fornitori, ecc.). Ai fini del presente documento, per evento di sicurezza si intende l'occorrenza dello stato di un sistema, servizio o rete che indichi una potenziale infrazione di una policy o il fallimento di un controllo, o il verificarsi di una situazione precedentemente ignota e potenzialmente rilevante per la tutela delle informazioni. Un incidente è costituito da un evento o una sequenza di eventi di sicurezza indesiderati che comportino una significativa probabilità di compromissione delle operazioni di business e della sicurezza delle informazioni, intesa come integrità, disponibilità e riservatezza del patrimonio informativo. L'occorrenza di un evento di sicurezza non comporta necessariamente la compromissione di integrità, disponibilità e/o riservatezza delle informazioni, pertanto non tutti gli eventi di sicurezza sono classificati come incidenti.

Un incidente di sicurezza può essere deliberato (es.: causato da codice malevolo o infrazioni intenzionali delle politiche di sicurezza) o accidentale (es.: causato da errori umani o fenomeni naturali). Le conseguenze possono includere diffusione non autorizzata, modifica, distruzione o indisponibilità di informazioni, oppure il danneggiamento o furto di asset aziendali che contengono informazioni, con impatti potenziali in termini di perdite finanziarie, interruzione dei servizi di business, danni reputazionali e sanzioni normative.

Di seguito si riporta, a titolo esemplificativo e non esaustivo, un elenco di possibili incidenti di sicurezza delle informazioni:

1. accessi non autorizzati a dati e risorse;
2. perdita di dati;
3. distruzione intenzionale o modifica di dati;
4. interruzione di servizi;
5. attacchi derivanti dall'utilizzo di codice malevolo;
6. compromissione dei privilegi di accesso a software/dati/sistemi;
7. intrusione o tentativo di intrusione da parte di attaccanti esterni;
8. violazione delle policy interne da parte di dipendenti;
9. violazione delle normative attualmente vigenti in materia di protezione dei dati e sicurezza delle informazioni.

9.3. Normative e standard di riferimento

La presente procedura recepisce le *best practice* e gli standard internazionali applicabili al contesto, al fine di assicurare uno svolgimento dell'operatività in linea con le più recenti e consolidate tecniche di gestione della sicurezza ICT. Essa disciplina altresì il processo di gestione degli incidenti di sicurezza delle informazioni in conformità alle normative vigenti applicabili. In particolare tali normative e standard risultano essere:

DPCM 27 gennaio 2014 – Strategia nazionale per la sicurezza cibernetica (Quadro strategico nazionale) Sostituito dal nuovo Piano nazionale adottato con DPCM 31 marzo 2017;

DPCM 17 febbraio 2017 – Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (Piano nazionale per la protezione cibernetica e la sicurezza informatica);

ISO/IEC 27001 – Information Technology – Security Techniques - Information Security Management Systems Requirements;

ISO/IEC 27035:2016 – Information Technology – Security Techniques - Information Security Incident Management;

ITIL v3 – Service Operations;

ENISA - Good Practice for Guide for Incident Management (2010);

SANS Institute – Incident handling handbook.

9.4. Attori coinvolti

Le attività previste in ambito alla gestione degli incidenti di sicurezza delle informazioni prevedono il coinvolgimento di molteplici attori, attivati nelle modalità e nelle tempistiche descritte dalla presente procedura. Nello specifico, tali attori includono:

- Utenti;
- ACI Informatica;
- ACI - Direzione Sistemi Informativi e Innovazione
- Comitato di Crisi.

Per ciascuno di essi, segue una breve descrizione dei principali compiti e responsabilità attribuiti.

9.4.1. Utenti

Gli utenti includono tutti i dipendenti e terze parti (e.g. dipendenti ACI, dipendenti ACI Informatica, consulenti, personale temporaneo, fornitori, ecc.) che hanno accesso al patrimonio informativo di ACI.

Ad essi è richiesto di registrare e segnalare qualsiasi evento o punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.

Gli utenti devono avere particolare cura di effettuare le segnalazioni in maniera tempestiva e fornendo le informazioni richieste, indicate nella presente procedura, nella maniera più accurata e completa possibile, al fine di consentire una diagnosi efficace ed efficiente dell'evento.

9.4.2. ACI Informatica

ACI Informatica, in quanto partner tecnologico di ACI e Responsabile esterno del trattamento informatizzato dei dati della suddetta, è responsabile per la gestione dell'intero ciclo di vita degli incidenti di sicurezza delle informazioni.

Le attività in carico ad ACI Informatica includono il monitoraggio delle sonde e degli strumenti di sicurezza proattiva, la presa in carico delle segnalazioni ricevute dagli utenti, la classificazione degli incidenti, nonché le attività di analisi e risposta. Essa inoltre è responsabile per la comunicazione e il reporting verso la Direzione Sistemi Informativi e Innovazione di ACI e del suo coinvolgimento in incidenti di particolare gravità, che possano richiedere decisioni strategiche da parte di quest'ultima o l'attivazione di particolari procedure di escalation (e.g. *Data Breach Notification*, *Crisis Management*).

9.4.3. ACI - Direzione Sistemi Informativi e Innovazione

In ambito gestione degli incidenti di sicurezza delle informazioni, la Direzione Sistemi Informativi e Innovazione di ACI viene coinvolta con ruolo consultivo e autorizzativo nella gestione degli incidenti di particolare severità. Di concerto con ACI Informatica è inoltre responsabile per la revisione della reportistica periodica, finalizzata a verificare la corretta applicazione della presente procedura, nonché la sua adeguatezza e miglioramento continuo.

La Direzione Sistemi Informativi e Innovazione invita tutto il personale ed i collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione a registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei medesimi.

Tali segnalazioni devono essere inoltrate alla casella *funzionesicurezzasi@aci.it*, presidiata dal personale dell'Ufficio Organizzazione Digitale di DSII.

9.4.4. Comitato di crisi

Il Comitato di crisi ha il compito di coordinare la risposta all'evento in modo strategico e tempestivo.

Sono Componenti del Comitato di crisi:

- il Presidente dell'Automobile Club d'Italia;
- il Segretario Generale dell'Automobile Club d'Italia:
- il Direttore Centrale Sistemi Informativi e Innovazione;
- il Direttore Centrale Presidenza e Segreteria Generale;
- il Consigliere per le Relazioni Esterne e Istituzionali;
- il Direttore Centrale Organizzazione e Gestione della Privacy e Monitoraggio del Sistema Qualità dell'Ente;
- il Data Protection Officer;

- il Direttore Centrale Risorse Umane e Organizzazione;
- il Direttore Centrale del Servizio coinvolto dall'incidente di sicurezza;
- il Direttore di Aci Informatica;
- il Vice Direttore di Aci Informatica;
- il Dirigente Ufficio per l'Organizzazione Digitale;
- il Responsabile Sicurezza Informatica ACI Informatica;
- il Responsabile dell'Ufficio Stampa;
- il Rappresentante dell'Avvocatura ACI.

Esso è responsabile per la gestione strategica e tattica della crisi, assumendosi le decisioni che hanno implicazioni strategiche, anche per il lungo periodo, definendo le priorità di intervento e mettendo a disposizione le risorse necessarie (anche economiche) in tempi brevi per supportarle.

Per le violazioni di sicurezza che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'Ente, trova applicazione la disciplina di dettaglio predisposta dall'Ente, in applicazione della normativa vigente in materia e, in questo, il Comitato di Crisi si assume l'onere di redigere la relazione al Garante della Privacy nel caso eventuale di data breach.

9.5. Gestione degli incidenti di sicurezza delle informazioni

Nella sua attività ACI Informatica è tenuta a:

- monitorare, rilevare e analizzare eventi anomali attraverso il controllo della rete della Federazione ACI;
- definire tutte le informazioni richieste in fase di segnalazione per consentire una diagnosi efficace ed efficiente dell'evento;
- valutare gli eventi rilevati stabilendo se classificarli come incidenti relativi alla sicurezza delle informazioni. I risultati di tale valutazione e classificazione devono essere registrati e conservati per riesame e verifica;
- pianificare e preparare delle azioni di risposta, ivi incluse le procedure di escalation (es.: *Crisis Management*);
- comunicare tempestivamente incidenti di sicurezza, specificando la natura dell'incidente: controlli di sicurezza non efficaci; perdita di riservatezza, integrità o disponibilità di un dato; errori umani; non-compliance a policy o linee guida; violazioni del sistema di sicurezza fisica; cambiamenti non controllati a sistemi; malfunzionamenti nel software o nell'hardware;
- tracciare le attività di gestione degli incidenti;
- conservare le evidenze ove appropriato (es.: nel caso di incidenti che possano avere rilevanza nell'ambito di futuri provvedimenti disciplinari o procedimenti legali);
- fornire alla Direzione Sistemi Informativi e Innovazione il report degli eventi anomali e degli eventuali incidenti di sicurezza delle informazioni;
- valutare eventuali debolezze nel sistema di controllo per colmarle attraverso appropriati aggiornamenti/evolutive;

- porre in essere, nell'interlocuzione con la Direzione Sistemi Informativi e Innovazione, un appropriato processo di feedback, finalizzato a garantire che le persone che segnalano un evento di sicurezza siano messe a conoscenza dei risultati derivanti dall'analisi della segnalazione;
- utilizzare la conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni per verificare la verosimiglianza e/o ridurre l'impatto degli incidenti futuri.

9.5.1. Fasi del processo di gestione incidenti

Il processo di gestione incidenti è articolato nelle seguenti attività:

- monitoraggio, a carico di Aci Informatica, finalizzato all'individuazione degli eventi rilevati automaticamente, ovvero alla ricezione delle segnalazioni di comportamenti anomali o sospetti;
- analisi e prima classificazione degli eventi di sicurezza;
- attivazione del sotto-processo di gestione degli allarmi o di gestione incidenti, coinvolgendo o meno il Comitato di crisi, in funzione del livello di classificazione e dell'eventuale rilevanza sistemica dell'incidente;
- monitoraggio delle attività di ripristino ed analisi post-incidenti.

9.5.2. Monitoraggio degli eventi di sicurezza

La responsabilità delle attività continuative H24 7x7 di monitoraggio degli incidenti di sicurezza è in carico Aci Informatica.

Il monitoraggio degli eventi di sicurezza consiste nelle seguenti attività:

- rilevazione delle segnalazioni prodotte in tempo reale dai dispositivi informatici di monitoraggio, cui è affidato il compito di tracciare e segnalare tutti gli eventi di sicurezza ICT occorsi nel dominio degli asset ICT controllati;
- analisi periodiche dei log prodotti dai dispositivi di monitoraggio o da altre piattaforme di sicurezza gestite, per il rilevamento di pattern sospetti e/o eventi ripetuti, che possano evidenziare attività malevoli;
- raccolta e valutazione delle comunicazioni, verbali o scritte, di comportamenti anomali o di eventi sospetti provenienti da utenti o amministratori di sistema;
- raccolta e valutazione delle comunicazioni (sotto forma di alert o bollettini di sicurezza) provenienti da fonti esterne autoritative circa nuovi scenari di rischio, comportamenti anomali o attacchi in corso ai danni di altri, che potrebbero avere impatto sul patrimonio tecnologico gestito.

9.6. Gestione dell'incidente

Segnalazione

L'incidente viene segnalato da utenti o sonde che rilevano anomalie o violazioni della sicurezza informatica.

Assessment

Dopo la segnalazione dell'incidente, viene eseguito da ACI Informatica un assessment per valutare la gravità e l'impatto dell'incidente sulla sicurezza.

Valutazione della gravità dell'Incidente

Se dall'assessment non risultano rischi in quanto l'evento è già gestito dalle ordinarie procedure, l'incidente viene gestito senza la necessità di coinvolgere la Direzione Sistemi Informativi e Innovazione.

Se l'assessment invece indica che l'incidente è grave, ACI Informatica informa la Direzione Sistemi Informativi e Innovazione.

In particolare, gli eventi di minore rischio vengono portati alla conoscenza del Dirigente dell'Ufficio per l'Organizzazione Digitale. Gli incidenti più gravi vengono invece segnalati immediatamente al Responsabile della Sicurezza Informatica di ACI.

La gestione dell'evento è demandata ad Aci Informatica per le azioni successive.

Valutazione Data Breach

Se l'assessment conferma un potenziale data breach, su segnalazione di ACI Informatica, il Responsabile della Sicurezza Informatica informa immediatamente il Data Protection Officer e il Direttore Centrale Organizzazione e Gestione della Privacy e Monitoraggio del Sistema Qualità dell'Ente dell'accaduto. Questo processo attiva la procedura di gestione delle violazioni dei dati.

Crisi

Se l'assessment non conferma un data breach ma l'incidente è considerato una Crisi, il Responsabile della Sicurezza Informatica di ACI convoca il Comitato di Crisi per avviare la gestione della situazione critica.

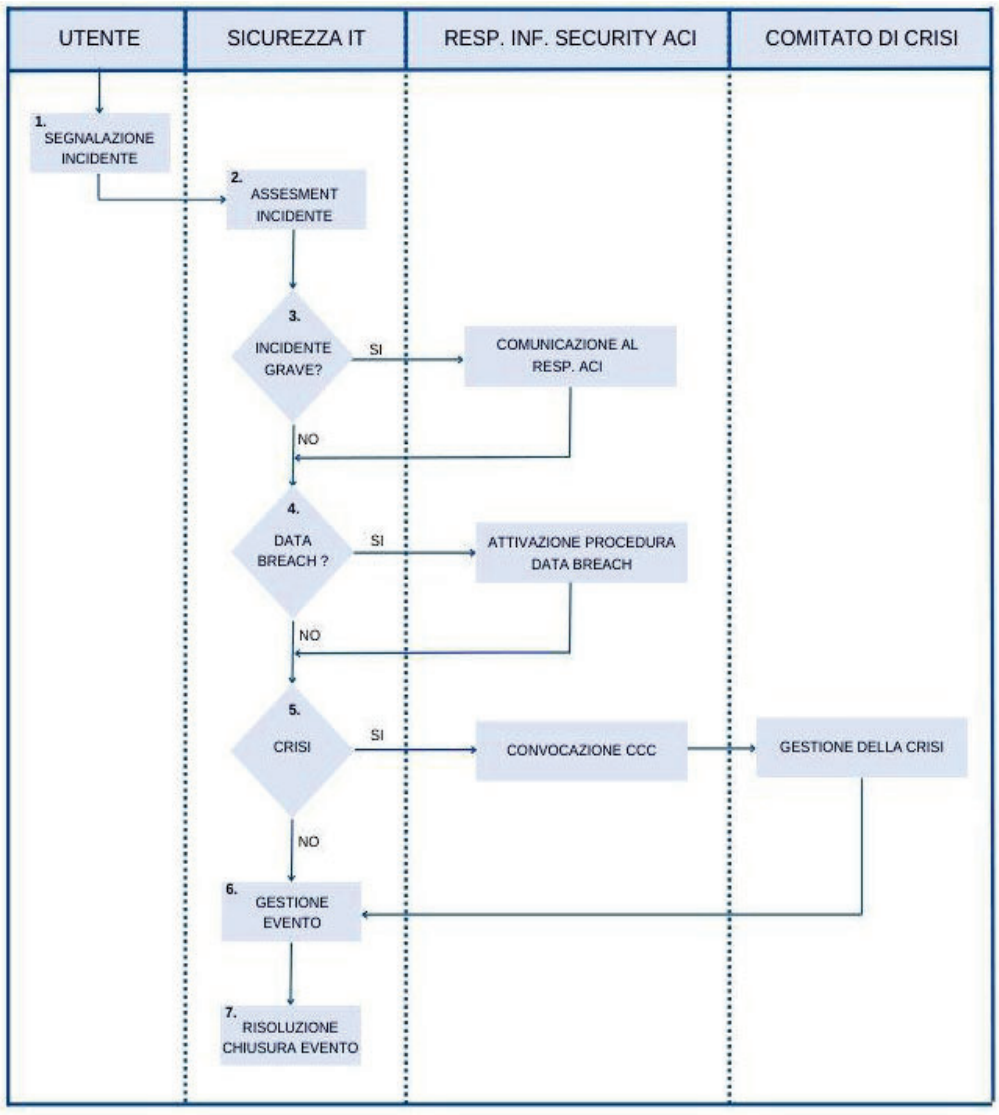
Gestione dell'Evento

Nel caso in cui l'assessment non confermi un data breach e l'incidente non sia classificato come una Crisi, ACI Informatica assume la responsabilità della gestione dell'evento.

Chiusura e Reporting

Dopo aver gestito con successo l'incidente, si procede alla fase di chiusura dell'evento.

Durante questa fase verrà redatto un report dettagliato che documenta l'intero processo di gestione dell'incidente. Una volta completato, il report sarà inviato al Responsabile della Sicurezza Informatica di ACI.



9.7. Tassonomia degli incidenti di sicurezza informatica

Tipologia incidente	**Descrizione**	**Effetti**	**Sintomi precursori**
Accesso non autorizzato	Attacco finalizzato ad ottenere accesso illecito alle risorse di un sistema IT, generalmente sfruttando vulnerabilità presenti in sistemi operativi, applicazioni e controlli di autenticazione e autorizzazione. Esempi di "Accesso non autorizzato" possono includere: accesso non autorizzato ai dati; password cracking; deturpazione di un sito web. L'attacco è generalmente preceduto da attività preparatorie che mirano ad ottenere informazioni sull'infrastruttura e sulle vulnerabilità esistenti, come ad esempio: trace route, port scan, vulnerability scan, OS fingerprinting, sniffing di pacchetti, ecc.; attività di "ingegneria sociale". Le tecniche di attacco includono intercettazione di password e dati e sfruttamento di bug nel software o nella configurazione dei sistemi.	Perdita di riservatezza, integrità e disponibilità dei dati. Compromissione di sistemi e asset.	Anomalie evidenziate da sistemi locali e /o centralizzati, log applicativi e dei sistemi di rete. Alert generati da IPS, IDS, SIEM. Violazioni di Access Control List di router / switch. Scansioni prolungate o frequenti di porte e servizi. Utilizzo anomalo o non autorizzato dei servizi. Utilizzo anomalo o saturazione delle risorse dei sistemi (e.g. CPU). Accesso o tentativi di accesso anomali ai password file. Rilevazione di multipli tentativi di accesso falliti (e.g. password errata). Crescita anomala nel numero di account bloccati. Crescita anomala nella dimensione dei file di log. Anomalie nella nomenclatura di file e directory.
Denial of Service (DoS)	Attacco mirato a provocare il blocco totale o parziale dei servizi erogati da un sistema IT, compromettendo l'utilizzo legittimo di reti, sistemi e applicazioni attraverso richieste continue di	Perdita di disponibilità dei dati Indisponibilità del sistema target Interruzione dei servizi applicativi Indisponibilità di un canale di	Alert generati da IPS, IDS. Anomalie rilevati nei log di router / firewall. Anomalie negli indirizzi sorgente / destinazione dei pacchetti di rete. Saturazione della rete e/o

Tipologia incidente	Descrizione	Effetti	Sintomi precursori
	elaborazione e/o di accesso, tali da sopraffare la potenza di elaborazione del sistema o la capacità del disco.	trasmissione.	delle risorse dei sistemi (e.g. CPU). Incremento notevole nei tempi di risposta di servizi / applicazioni.
Virus / Codice malevolo	Incidente connesso alla diffusione di codice malevolo (o malware), ovvero software creato con il solo scopo di arrecare danni più o meno gravi al sistema su cui è eseguito. I tipi principali di malware includono: ● Virus ● Worm ● Cavallo di Troia ● Backdoor ● Spyware	Perdita di riservatezza, integrità e disponibilità dei dati. Decremento nelle performance di sistemi, applicazioni e reti. Inclusione degli IP pubblici di ACI/ACI Informatica su blacklist.	Alert generati dai sistemi antivirus. Alert generati da IPS, IDS, SIEM. Comportamento anomalo di reti e sistemi. Tempistiche anomale di start- up/risposta di sistemi, applicazioni e servizi. Ricezione di e-mail con allegati anomali. Presenza di icone sconosciute sui sistemi Sparizione di file e programmi sui sistemi. Impossibilità di eseguire il boot dei sistemi operativi. Instabilità e crash continui dei sistemi. Perdita di dati. Uso eccessivo o sovraccarico delle risorse dei sistemi (e.g. CPU). Saturazione dello spazio disco. Modifica della home page o apparizione di banner frequenti nel corso della navigazione internet. Alert generati da servizi pubblici di blacklist
Utilizzo illecito delle risorse (sistemi, infrastrutture, informazioni)	Incidente di sicurezza derivante dall'accesso legittimo a informazioni e risorse aziendali e finalizzato a: - utilizzo improprio o non autorizzato o diffusione di	Perdita di riservatezza, integrità e disponibilità dei dati. Compromissione di sistemi e asset.	Anomalie nell'utilizzo di informazioni e risorse dell'Ente evidenziate da log locali e/o centralizzati afferenti a sistemi, applicazioni e reti. Alert generati da IPS,

Tipologia incidente	**Descrizione**	**Effetti**	**Sintomi precursori**
	dati accessibili in relazione al proprio ruolo all'interno dell'Ente; - utilizzo di risorse aziendali (sistemi e infrastruttura) per scopi che non fanno parte di politiche aziendali e / o per fini illeciti.		IDS, SIEM. Modifiche alla configurazione di sistemi, applicazioni e reti. Evidenze derivanti da investigazioni foresti interne o esterne. Attività anomale rilevate da sistemi di videosorveglianza nelle aree ad accesso limitato.
Furto o perdita di informazioni	Incidente di sicurezza derivante dalla raccolta o distribuzione di informazione dell'Ente di carattere non pubblico.	Perdita di riservatezza e disponibilità dei dati.	Alert di terze parti (e.g. CNAIPIC) Monitoraggio di fonti pubbliche.
Phishing	Frode informatica che impatta la reputazione o l'immagine dell'Ente.	Danno reputazionale.	Alert di fonti interne o esterne.
Altro	Incidenti che non ricadono nelle precedenti categorie.	Da valutare caso per caso	Eventi sospetti che non possono essere identificati o classificati nelle precedenti categorie.

10. Sanzioni

La violazione delle disposizioni di servizio relative al corretto uso delle applicazioni e dei dispositivi in dotazione determina responsabilità disciplinare.

Qualora la violazione integri altresì gli estremi indicati delle fattispecie di cui agli artt. 615 ter, quater e quinquies del Codice Penale, determina altresì la denuncia alle competenti Autorità per gli accertamenti ai sensi delle norme di legge.

Art. 615-ter.

Accesso abusivo ad un sistema informatico o telematico.

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Art. 615-quater.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Art. 615-quinquies. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Con particolare riferimento alla tutela dei Dati personali, l'omessa adozione delle misure di sicurezza di cui all'art. 32 del GDPR, comporta l'irrogazione delle sanzioni amministrative pecuniarie di cui all'art. 83 del citato Regolamento.