TECHNICAL REPORT

IIT TR-01/2021

Policy di sicurezza informatica dell'Istituto di Informatica e Telematica

A. De Vita, A. Gebrehiwot, F. Lauria, C. Lucchesi, A. Mancini,
M. Martinelli, C. Porta, S. Ruberti, L. Vasarelli

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

Technical Report

Policy di sicurezza informatica dell'Istituto di Informatica e Telematica

Autori:

De Vita Andrea, Gebrehiwot Abraham, Lauria Filippo, Lucchesi Cristian, Mancini Alessandro, Martinelli Maurizio, Porta Claudio, Ruberti Stefano, Vasarelli Luca

Abstract

Questo technical report riporta la prima versione della Security Policy dell'Istituto di Informatica e Telematica, adottata nel rispetto della normativa vigente "Misure minime di sicurezza ICT per le pubbliche amministrazioni" previste dall'Agenzia per l'Italia Digitale. Tratta gli aspetti necessari per rilevare eventuali criticità di sicurezza informatica e stabilisce le azioni da intraprendere per accrescere il livello di sicurezza dell'intero ecosistema informatico dell'Istituto. Definisce inoltre un insieme di misure organizzative e comportamentali da adottare, da parte del personale dello IIT, per contrastare le minacce informatiche più frequenti e gestire eventuali incidenti.

Un ulteriore obiettivo è la consultazione e divulgazione della policy stessa ad altri istituti del CNR, enti di ricerca e Pubblica Amministrazione, al fine di supportarli nella definizione di una politica di sicurezza per la propria organizzazione.

Keywords. Security Policy, Vulnerability Assessment, AGID, Access Control, Incident response

1. Introduzione

Avendo maturato un alto grado di consapevolezza del rischio informatico, l'Istituto di Informatica e Telematica (IIT) ha deciso di redigere la presente policy di sicurezza. Quest'ultima costituisce un insieme di misure organizzative e comportamentali da adottare per tutelare le risorse informatiche dell'Istituto e gestire gli eventuali incidenti ad esse relativi.

Pertanto, la policy si applica all'utilizzo e alla gestione della rete, dei servizi informatici e delle apparecchiature connesse in rete, da parte del personale strutturato[1] e non strutturato[2] dello IIT, il quale si impegna a rispettare quanto in essa contenuto, nonché quanto stabilito dalle vigenti norme di legge e regolamenti in materia di sicurezza informatica.

La policy è un documento pubblico ed è conforme alle misure minime di sicurezza ICT per le pubbliche amministrazioni emanate dall'AgID[3]. Inoltre, essa sarà periodicamente aggiornata al fine di rimanere efficace e coerente con l'evoluzione tecnologica e normativa. Tutto il personale dello IIT sarà formato adeguatamente per assumere un comportamento responsabile in termini di sicurezza informatica nel rispetto della policy. Per questo motivo, è prevista l'organizzazione periodica di eventi di formazione sulle pratiche ed i comportamenti che il personale IIT deve osservare.

Chiunque sia coinvolto nell'uso e nella gestione delle risorse d'Istituto deve formalmente accettare quanto in essa contenuto, firmando l'apposito modulo di accettazione (*"Modulo di accettazione della policy di sicurezza"*).

2. Risorse informatiche dell'Istituto

Il personale IIT coinvolto nell'uso e nella gestione di risorse informatiche può rivestire vari ruoli:

- **gestore** - gode del livello massimo di privilegio consentito per lo svolgimento delle operazioni eseguibili su una risorsa;
- **utilizzatore** - ha privilegi limitati per lo svolgimento di determinate operazioni eseguibili su una risorsa.

Una risorsa informatica deve avere almeno un gestore e può avere uno o più utilizzatori. Uno stesso soggetto può ricoprire entrambi i ruoli. Nello svolgere operazioni che richiedono il livello massimo di privilegio consentito su laptop o workstation (ad esempio prima configurazione, installazione di driver, ecc.), un utilizzatore può avvalersi del supporto di un apposito ufficio che riveste il ruolo di gestore di quel dispositivo.

[1] con personale strutturato si intendono tutti i dipendenti con matricola CNR
[2] con personale non strutturato si intendono tutti i collaboratori, borsisti, assegnisti, dottorandi, tirocinanti/project work, partner di progetto, ERCIM.
[3] Agenzia per l'Italia Digitale https://www.agid.gov.it/

Per un periodo di tempo limitato ed in contesti ben circoscritti (ad esempio: partner di progetti di ricerca, supporto tecnico remoto, ecc.), previa autorizzazione del Direttore e accettazione della presente policy, può essere concesso a terze parti il ruolo di gestore per accedere ad una risorsa di Istituto.

Inoltre, esistono appositi ruoli per la gestione delle risorse informatiche infrastrutturali e strategiche d'Istituto:

- **gestori di rete** - il personale coinvolto nella gestione dell'infrastruttura di rete e delle problematiche di sicurezza, derivanti dalle minacce informatiche ad essa relative;
- **gestori dei servizi** - il personale coinvolto nella gestione dei servizi informatici dello IIT e delle relative problematiche di sicurezza.

Raggiungere e mantenere un adeguato livello di sicurezza informatica in Istituto costituisce un unico processo svolto in maniera collaborativa da tutti i soggetti precedentemente menzionati. Pertanto, è compito di ciascuno di essi osservare comportamenti consoni alla policy di sicurezza ed attuare misure necessarie per svolgere efficacemente tale processo.

L'infrastruttura informatica dell'Istituto è costituita dalle seguenti principali tipologie di risorse:

- infrastruttura di rete;
- dati sensibili;
- servizi informatici;
- software;
- dispositivi informatici.

2.1. Infrastruttura di rete

L'infrastruttura di rete dell'Area della Ricerca di Pisa è composta da un insieme di apparati interconnessi tra loro ed è segmentata in differenti sottoreti. Il backbone L2, gli apparati di rete (router e firewall) e le loro interconnessioni sono ridondate in modo da evitare disservizi in caso di malfunzionamento di una singola componente hardware. Il livello di accesso non è ridondato, ma esistono apparati di scorta e backup di configurazioni per la rapida sostituzione in caso di guasti.

La rete dello IIT fa parte di questa infrastruttura ed è suddivisa nelle quattro sottoreti seguenti:

- sottorete degli utenti;
- sottorete dei servizi di Istituto;
- sottorete per attività di ricerca e sviluppo;
- sottorete per attività di ricerca e sviluppo - partner.

Gli ospiti e i visitatori dell'Istituto che hanno la necessità di accedere ad Internet possono collegare i propri dispositivi alla "sottorete degli ospiti", una rete wireless appartenente all'Area della Ricerca di Pisa.

Informazioni più dettagliate sull'utilizzo, sullo scopo e sulla gestione di tali sottoreti sono specificate nel paragrafo "*Protezione della rete*".

2.2. Dati sensibili

Sono considerati dati sensibili tutte le informazioni che in base alla loro valenza, riservatezza ed importanza non devono essere resi pubblici. A questa categoria appartengono i dati che identificano o rendono identificabile una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

2.3. Servizi informatici

L'Istituto dispone di un elevato numero di servizi informatici di utilità generale per lo svolgimento delle attività, previsti da organigramma e mansionario, per i quali è ben identificata la figura del relativo gestore, facente parte dell'organico della struttura.

Alcuni sono rivolti esclusivamente al personale IIT (posta elettronica, mailing list, VPN, ePAS, sistema di condivisione dei documenti, ecc.), mentre altri sono pubblici (sito web d'Istituto, DNS, ecc.). L'elenco dei servizi rivolti al personale IIT è consultabile nell'apposita sezione del sito web d'Istituto.

L'Istituto inoltre offre dei servizi ad altre pubbliche amministrazioni e istituti del CNR, come ad esempio DNS, posta elettronica, mailing list, hosting di siti Web, ePAS, ecc. Questi ultimi sono regolamentati da apposite collaborazioni scientifiche o convenzioni.

Infine esistono servizi erogati e gestiti dalle varie unità di ricerca e tecnologiche.

2.4. Software

Nell'ambito della presente policy, il termine *risorsa software* indica l'insieme dei programmi che gestiscono e specializzano il funzionamento di un elaboratore, nonché le dipendenze necessarie per la loro esecuzione.
Esempi di *risorse software* sono: sistemi operativi, programmi commerciali, programmi che non richiedono l'acquisizione di una specifica licenza d'uso[4], software sviluppato dal personale IIT, ecc.

Oltre a quanto detto, la policy, nel paragrafo *"Uso del software",* regolamenta anche l'uso di *codice sorgente* e *librerie di sviluppo software* reperibili in rete.

2.5. Dispositivi informatici

Per dispositivi informatici, sia fisici che virtuali, si intendono:

[4] ad es. open source, freeware, ecc.

- i laptop e le workstation usate da dipendenti e collaboratori;
- i server fisici;
- le macchine virtuali;
- le stampanti posizionate negli spazi comuni o negli uffici del personale;
- i dispositivi di archiviazione dati connessi in rete (NAS, Network Attached Storage);
- ulteriori apparati (smartphone, tablet, ecc.) con capacità di connessione in rete che il personale ha in dotazione dallo IIT;
- i dispositivi di archiviazione quali hard disk esterni, penne USB su cui ad esempio vengono fatti backup o che sono utilizzati per lo scambio di file all'interno dell'Istituto.

3. Protezione delle risorse informatiche

In questa sezione vengono trattate le strategie e le procedure atte ad accrescere il livello di sicurezza informatica delle risorse di Istituto.

3.1. Assegnazione dei dispositivi informatici

Il processo di assegnazione dei dispositivi informatici al personale IIT consente di stabilire un legame tra *dispositivo*, *gestori* ed *utilizzatori*, in modo da definire un criterio di responsabilità basato sul ruolo di ogni soggetto coinvolto. Tale processo è strettamente legato alla fase di collaudo e successiva fase di inventario dei dispositivi ed è effettuato da appositi uffici. Per tale ragione questo passo diventa indispensabile per ogni nuovo dispositivo informatico che entra in Istituto.

Tutti i dispositivi personali non di proprietà dello IIT, devono essere autorizzati dal Direttore prima di essere connessi alle reti d'Istituto. Anche in questo caso, il soggetto si impegna a rispettare quanto stabilito dalla presente policy.

3.2. Controllo degli accessi

Il controllo degli accessi è una componente fondamentale della sicurezza dei dati e dell'infrastruttura informatica e consente di stabilire chi ha i diritti di accesso e di utilizzo delle risorse informatiche dell'Istituto. Attraverso meccanismi di autenticazione e autorizzazione, le policy di controllo degli accessi verificano l'identità degli utenti e garantiscono l'accesso appropriato ai sistemi, alle applicazioni e ai dati.

3.2.1. Accesso a risorse protette

Con il termine risorsa protetta si intende una risorsa informatica che, tramite un meccanismo di controllo degli accessi adottato dal rispettivo gestore, è disponibile solamente ai soggetti autorizzati.

3.2.1.1. Autenticazione

L'accesso alle risorse protette che richiedono l'autenticazione da parte dell'utilizzatore deve avvenire mediante la verifica dell'identità di quest'ultimo (ad esempio tramite username e password, certificati digitali, parametri biometrici, ecc.). Le attività informatiche eseguite su tali risorse devono poter essere riconducibili ad un account personale. Ad ogni modo, sia il gestore che l'utilizzatore devono rispettare quanto specificato nel documento "*Politiche di utilizzo delle credenziali di accesso*".

3.2.1.2. Autorizzazione

Il processo di autorizzazione permette di assegnare agli utilizzatori adeguati privilegi di accesso alle risorse informatiche. È compito del gestore definire una politica di accesso conforme con le seguenti linee guida:

- garantire ai soli soggetti autorizzati il privilegio minimo per svolgere una determinata operazione e verificare che l'accesso sia negato a tutti gli altri soggetti;
- verificare che i privilegi assegnati restino coerenti nel tempo.

È compito del gestore della risorsa definire i meccanismi per la gestione del controllo degli accessi e strutturare la politica di accesso alla risorsa, categorizzando ove possibile i soggetti in gruppi piuttosto che gestirli singolarmente. Ad esempio, risorse comuni come le stampanti possono essere utilizzate da tutto il personale collegato alla rete IIT, dati condivisi da un gruppo di utilizzatori mediante un NAS devono essere accessibili solo dai componenti di quel gruppo, ecc.

3.2.1.3. Accounting

È compito del gestore della risorsa tenere traccia degli accessi e, ove possibile, delle informazioni di utilizzo della risorsa protetta. I log prodotti devono contenere, oltre ad un riferimento temporale valido, tutte le informazioni necessarie all'individuazione delle azioni intraprese e chi le ha intraprese. Per consentire la consistenza temporale, gli orologi dei dispositivi devono essere sincronizzati, quando possibile, con un servizio NTP affidabile (ad esempio: it.pool.ntp.org).

Si noti infine che le informazioni contenute nei file di log devono essere utilizzate esclusivamente per la verifica del corretto funzionamento del servizio e delle sue politiche di accesso, nel rispetto delle norme sulla privacy e sulla tutela del lavoratore.

3.2.2. Accesso alla rete

Tutte le sottoreti d'Istituto, anch'esse considerate risorse protette, prevedono appositi meccanismi di controllo, i quali consentono l'accesso solamente ai dispositivi di proprietà dell'Istituto, preventivamente collaudati e inventariati, o dispositivi personali autorizzati, come ad esempio nel caso di un assegnista col proprio PC. Come già menzionato nel paragrafo *"Infrastruttura di rete"*, gli ospiti e i visitatori dell'Istituto che hanno la necessità di accedere ad Internet possono collegare i propri dispositivi esclusivamente alla "sottorete degli ospiti".

Gli utenti che hanno esigenze di collegarsi da remoto alle sottoreti possono farlo attraverso il servizio VPN messo a disposizione dai gestori di rete. In questo modo, l'utente remoto può utilizzare i servizi disponibili con le stesse modalità rispetto a quando connesso localmente alla sottorete. Si noti che le credenziali utilizzate per l'accesso da remoto devono rispettare quanto stabilito nel documento *"Politiche di utilizzo delle credenziali di accesso"*. Non essendo implementato nessun meccanismo di controllo dei dispositivi connessi tramite VPN, è responsabilità degli utenti garantire che l'accesso avvenga solo attraverso un dispositivo autorizzato dall'Istituto.

3.3. Protezione dalle minacce informatiche

I gestori di rete e i gestori dei servizi utilizzano vari strumenti software per rilevare eventuali problemi di sicurezza dei sistemi connessi in rete. Lo scopo è quello di aumentare la sicurezza informatica, correggendo, ove possibile, eventuali problemi rilevati e/o applicando protezioni ai sistemi vulnerabili.

3.3.1. Valutazione e correzione continua delle vulnerabilità in rete

Sia i gestori di rete che i gestori dei servizi utilizzano sistemi IDS/IPS, network scanner, firewall e strumenti per il Vulnerability Assessment, in grado di produrre report contenenti indicazioni sulla criticità delle vulnerabilità scoperte. Questi strumenti devono a loro volta essere mantenuti aggiornati in modo da individuare nuove minacce. Le informazioni provenienti dai report vengono analizzate e correlate al fine di individuare ulteriori criticità non rilevate automaticamente. È compito dei gestori di rete, una volta rilevata una criticità, applicare eventuali filtraggi del traffico per mitigarne gli effetti e segnalare il problema ai gestori dei sistemi vulnerabili fornendo, ove possibile, dettagli utili alla risoluzione del problema.

I gestori e gli utilizzatori dei sistemi per i quali è stata riscontrata la vulnerabilità si impegnano ad applicare contromisure adeguate alla risoluzione del problema, eseguendo anche opportune verifiche per assicurarsi che le contromisure applicate siano state efficaci.

I sistemi vulnerabili per i quali non esiste alcuna contromisura nota devono essere disconnessi dalla rete, a meno di casi ritenuti eccezionali nei quali il gestore o l'utilizzatore hanno ricevuto adeguata autorizzazione del Direttore all'utilizzo del dispositivo, dopo aver verificato che la vulnerabilità in questione non rischia di compromettere altri servizi e/o risorse dell'Istituto. In tal caso il gestore o l'utilizzatore si assumono la responsabilità dell'azione svolta. Tali dispositivi saranno comunque filtrati dai firewall di frontiera.

3.3.1.1. Gestione del rischio

La gestione del rischio informatico è trattata nel documento *"Piano di Gestione del rischio informatico"*.

3.3.2. Protezione dei dati

La trasmissione, l'utilizzo e l'archiviazione dei dati sensibili deve essere implementata mediante l'uso di procedure che garantiscano la sicurezza dei dati. Nei casi in cui queste operazioni non siano possibili per limiti tecnici , rimane comunque necessaria l'adozione di opportune contromisure di sicurezza per garantire l'integrità e la sicurezza dei dati.

3.3.3. Protezione dei sistemi endpoint

Al fine di garantire un livello adeguato di sicurezza, la gestione e la configurazione di tutti i dispositivi, nuovi o attualmente in uso, devono essere conformi a quanto specificato nel documento "*Configurazioni standard, minime e sicure dei sistemi operativi*".

3.3.4. Protezione dei servizi informatici

La predisposizione, la configurazione e la verifica delle opportune politiche di sicurezza applicate ai servizi sono demandate ai relativi gestori. Tutte le politiche di sicurezza adottate sono volte all'integrità e alla protezione del servizio erogato e dei dati in esso gestiti.

Di seguito viene presentato un elenco non esaustivo delle azioni che un gestore di un generico servizio deve implementare:

- effettuare operazioni di management remoto del servizio utilizzando esclusivamente protocolli sicuri;
- non utilizzare software deprecati, avendo cura di mantenere aggiornato il servizio;
- ove possibile, installare periodicamente gli aggiornamenti di sicurezza;
- verificare la presenza di vulnerabilità ed eventualmente correggerle, in modo da accrescere il livello di protezione del servizio;

- in accordo alla tipologia di servizio, adottare funzionalità specifiche per aumentare il livello di protezione da minacce informatiche; ad esempio:
    - adottare meccanismi di protezione da attacchi di tipo DoS;
    - implementare meccanismi di mitigazione dei tentativi di autenticazione brute force;
    - avvalersi di software antivirus e antispam per server di posta;
- disabilitare l'esecuzione di applicazioni non necessarie;

Oltre a questo, per i servizi informatici di particolare importanza (ad esempio i servizi necessari per lo svolgimento delle attività di Istituto), l'elenco minimale delle azioni da intraprendere deve comprendere:

- ove possibile, implementare sistemi di ridondanza, sia hardware che software, in modo da minimizzare le interruzioni di servizio;
- effettuare periodicamente, con frequenza almeno settimanale, il backup dei dati e delle configurazioni, al fine di poter ripristinare la piena operatività del servizio in caso di necessità;
- implementare procedure di segnalazione di guasti o malfunzionamenti;
- interagire con i gestori di rete per implementare una politica di protezione del servizio sul firewall perimetrale;
- mantenere una documentazione aggiornata che descriva il funzionamento, la configurazione e le caratteristiche del servizio;
- attivare meccanismi di logging per verificare il corretto utilizzo dei servizi.

3.3.5. Protezione della rete

Come menzionato nel paragrafo "Infrastruttura di rete", la rete IIT è segmentata in quattro differenti sottoreti, ognuna delle quali con un proprio indirizzamento IPv4 e IPv6 e con specifiche politiche di firewalling. Inoltre, su tutte le sottoreti sono applicate almeno le seguenti politiche di filtraggio del traffico:

- traffico da Internet verso le sottoreti:
    - blocco dei protocolli deprecati;
    - filtraggio dei protocolli intrinsecamente insicuri, ovvero che non implementano sufficienti misure di sicurezza nello scambio delle informazioni (ad esempio FTP, Telnet e protocolli analoghi);
    - blocco di protocolli usati per fornire servizi VPN o proxy[5] non autorizzati;
- traffico dalle sottoreti verso Internet e viceversa:
    - blocco di virus, spyware e malware sul traffico non cifrato;
    - blocco di host malevoli, mediante l'utilizzo di blacklist pubbliche autorevoli;
    - threat prevention e mitigazione degli attacchi noti come ad esempio: DoS, brute force, ecc.;

[5] Come ad esempio OpenVPN, HTTP Proxy, SOCKS, ecc.

- filtraggio di applicazioni in grado di compiere azioni potenzialmente dannose come ad esempio: host sweep, port scan, ecc.

Ogni sistema connesso alle sottoreti di Istituto deve essere conforme a quanto stabilito nel documento "*Configurazioni standard, minime e sicure dei sistemi operativi*". Inoltre, tutti gli utenti si impegnano a collaborare con i gestori di rete al fine di garantire il corretto funzionamento della rete.

Gli strumenti di monitoraggio e gli apparati di rete sono utilizzati, nel rispetto delle vigenti norme di legge e regolamenti in materia di sicurezza informatica, per raccogliere informazioni riguardanti esclusivamente il funzionamento della rete e per contrastare e prevenire rischi informatici. Oltre alle informazioni raccolte, i gestori di rete ricevono le segnalazioni riguardanti comportamenti anomali[6] rilevati da soggetti esterni[7], che interessano i sistemi connessi ad una delle sottoreti dell'Istituto.

Di seguito sono descritte le politiche di sicurezza specifiche per ciascuna sottorete.

3.3.5.1. Sottorete degli utenti

Questa sottorete fornisce connettività a tutti i dispositivi informatici del personale strutturato e non può essere usata per fornire servizi di rete alla comunità Internet. I dispositivi tipicamente connessi sono:

- laptop e workstation;
- macchine virtuali;
- stampanti;
- dispositivi di archiviazione dati, come ad esempio i NAS.

Tutti i dispositivi devono essere collegati direttamente via cavo. I NAS possono essere utilizzati esclusivamente per consentire le operazioni di backup e/o come espansione di spazio disco e in nessun modo devono offrire servizi diversi da quelli comunemente utilizzati per il salvataggio dei dati, come per esempio DHCP.

In questa sottorete sono applicate politiche di firewalling che:

- consentono l'accesso ad Internet a tutti i dispositivi;
- bloccano tutte le connessioni originate da Internet verso i dispositivi.

3.3.5.2. Sottorete dei servizi di Istituto

Questa sottorete offre connettività ai servizi ufficiali d'Istituto. Tramite *politiche di firewalling basate su whitelist,* permette l'accesso da Internet ai soli servizi esposti e a servizi di management remoto mediante protocolli intrinsecamente

[6] Copyright infringement, vulnerabilità note, ecc.
[7] GARR-CERT, blocklist.de, ecc.

sicuri. L'accesso ad Internet è consentito a tutti i dispositivi connessi a tale sottorete.

3.3.5.3. Sottorete per ricerca e sviluppo

Questa sottorete è dedicata alle attività di ricerca, sperimentazione e sviluppo software del personale e pertanto ad essa sono connesse le risorse (ad esempio di calcolo, storage, ecc.) delle unità tecnologiche e di ricerca.

L'allegato "*Politiche di utilizzo delle risorse informatiche per il personale non strutturato*" descrive i diritti di accesso alle risorse informatiche da concedere al personale non strutturato IIT, contiene inoltre la modulistica necessaria per il loro utilizzo.

Per agevolare il lavoro agli eventuali collaboratori esterni (ad esempio partner di progetto, ecc.), i sistemi connessi a questa sottorete sono raggiungibili anche da Internet. Tramite politiche di firewalling basate su blacklist, alcuni protocolli (ad esempio DNS, SMTP, NTP, ecc.) sono bloccati sul firewall di frontiera.

In caso di motivata necessità, un utente può connettere un proprio dispositivo personale e non inventariato a tale rete previa formale autorizzazione del Direttore.

In ogni caso l'utente deve assumersi tutte le responsabilità nell'utilizzo della rete e i dispositivi connessi dovranno rispettare i requisiti di sicurezza della presente policy. Come meglio specificato nel paragrafo "Policy Compliance", eventuali necessità dell'utente non conformi o non previste dalla policy, come ad esempio collegare dispositivi che possono potenzialmente causare problemi di sicurezza, dovranno essere discusse e concordate con i gestori di rete.

3.3.5.4. Sottorete per ricerca e sviluppo - partner

Tale sottorete è dedicata esclusivamente ad attività di ricerca e tecnologiche (sperimentazione, sviluppo software, ecc.) che coinvolgono anche soggetti esterni all'Istituto. È concepita per facilitare la cooperazione tra enti di ricerca eterogenei, e favorire la gestione di risorse condivise. Il rilascio di eventuali credenziali di amministrazione a partner esterni richiede l'autorizzazione del Direttore.

Per quanto concerne la sicurezza, la politica di firewalling è di tipo whitelist, una strategia restrittiva che, tramite esplicita richiesta ai gestori del firewall, permette l'accesso via internet ai soli servizi esposti e il management remoto tramite protocolli intrinsecamente sicuri.
Le connessioni originate da questa rete verso le altre sottoreti IIT sono trattate allo stesso modo di quelle provenienti da Internet.
L'allegato "*Politiche di utilizzo delle risorse informatiche per il personale non strutturato*" descrive i diritti di accesso alle macchine fisiche e virtuali da concedere al personale non strutturato IIT, contiene inoltre la modulistica necessaria per il loro utilizzo.

3.3.5.5. Sottorete degli ospiti

Come già menzionato precedentemente, questa sottorete non appartiene all'insieme delle reti IIT, ma è un accesso wireless d'Area dedicato alla connettività Internet per gli ospiti degli istituti dell'Area della Ricerca del CNR di Pisa.
Ad essa si accede tramite utilizzo di credenziali e sono applicate politiche di firewalling che:

- consentono l'accesso ad Internet a tutti i dispositivi, applicando filtraggi che garantiscono l'utilizzo dei servizi base come ad esempio web, posta elettronica, ecc.;
- bloccano tutte le connessioni originate da Internet verso i dispositivi.

Le connessioni originate da questa rete verso le sottoreti IIT sono trattate allo stesso modo di quelle provenienti da Internet.

3.4. Uso del software

In questo paragrafo viene riportato un elenco non esaustivo di accorgimenti necessari per l'utilizzo delle "*risorse software*", del *"codice sorgente"* e delle *"librerie di sviluppo software"*.

Per tutte le categorie citate precedentemente valgono le seguenti assunzioni:

- nel caso in cui il software richieda una licenza d'uso, questa dev'essere ottenuta attraverso canali ufficiali (rivenditore, apposito ufficio di Istituto, ecc.);
- ove possibile, deve sempre essere utilizzata la versione software più recente e in ogni caso non contenente vulnerabilità note;
- le versioni utilizzabili sono esclusivamente quelle mantenute dal produttore e per cui vengono ancora rilasciati aggiornamenti di sicurezza.

Per le *risorse software*:

- è consentita esclusivamente l'esecuzione di software ottenuto attraverso canali ufficiali e indicato nella *"Lista dei software autorizzati"*, documento che verrà costantemente aggiornato coerentemente con l'evoluzione tecnologica e le esigenze di utilizzo del personale.

Per le *librerie di sviluppo software* e il *codice sorgente*:

- è consentito l'utilizzo di librerie o software reperibili su internet limitando il loro uso nell'ambito di tutte quelle attività che prevedano lo sviluppo di software da parte del personale IIT;
- è responsabilità del ricercatore/sviluppatore verificare che il codice sorgente e le librerie utilizzate non contengano vulnerabilità di sicurezza note;
- è responsabilità di chi sviluppa o utilizza il codice sorgente garantire che questo non introduca volontariamente vulnerabilità di sicurezza o arrechi danno ad altri.

In caso di necessità di utilizzo di software con vulnerabilità note oppure non conforme con quanto stabilito nella policy, occorre fare riferimento al paragrafo "*Policy Compliance*".

3.5. Trasferimento dei dispositivi all'esterno del perimetro dell'Istituto

Gli utenti possono portare, per necessità lavorative, i dispositivi all'esterno del perimetro dell'Istituto compilando l'apposito modulo di richiesta reperibile sul sito della intranet di Istituto.

Le configurazioni dei dispositivi autorizzati ad un uso esterno devono rispettare quanto contenuto nel paragrafo *"Protezione dei sistemi endpoint"*. Inoltre gli utilizzatori di tali dispositivi devono rispettare le seguenti linee guida:

- configurare la modalità di blocco automatico dell'accesso al sistema dopo un breve periodo di inattività o bloccare manualmente l'accesso al sistema quando il dispositivo non è in uso;
- utilizzare connessioni Internet di fiducia, adeguatamente protette (ad esempio evitare collegamenti a reti Wi-Fi pubbliche);
- utilizzare esclusivamente dispositivi removibili (pen drive, hd esterni, ecc.) di cui si conosce la provenienza;
- effettuare sempre il logout dai servizi Web una volta terminata la sessione lavorativa.

3.6. Trasferimento dati del personale a terze parti

È necessario richiedere l'autorizzazione del Direttore prima di eseguire una qualsiasi operazione di trasferimento di dati riguardanti il personale d'Istituto verso terze parti.

3.7. Uso di infrastrutture di virtualizzazione

È consentito l'utilizzo di infrastrutture per la virtualizzazione di risorse informatiche come server, storage, reti per l'erogazione di servizi, ecc.
È responsabilità degli amministratori:

- mantenere l'infrastruttura aggiornata;
- applicare tutte le misure di sicurezza relative all'infrastruttura nel suo complesso (backup, ridondanza, aggiornamenti di sicurezza, politica di utilizzo delle password, prima installazione, ecc);
- mantenere una documentazione aggiornata dell'infrastruttura, riguardante le modalità di utilizzo, la manutenzione e la gestione;
- mantenere l'archivio relativo alla gestione e all'utilizzo delle risorse virtualizzate (macchine virtuali e relativo gestore, servizi, password, ecc.) come descritto nel paragrafo 3.7.1.

Tali infrastrutture ereditano le regole di firewalling corrispondenti alle sottoreti su cui sono ospitate.

L’armonizzazione delle attuali infrastrutture presenti in Istituto sarà affrontata nelle prossime release del documento di policy, così come le relative politiche di sicurezza ed utilizzo.

3.7.1. Tipologie di risorse virtualizzate

Si distinguono due tipologie principali di risorse virtualizzate, *stabili* e *effimere*.

Per risorse *stabili* si intendono macchine virtuali utilizzate a tutti gli effetti come macchine fisiche, per scopi di ricerca, sviluppo o per ospitare servizi. Tali risorse hanno tipicamente un tempo di vita significativamente lungo, nell’ordine di mesi o anni, e hanno politiche di controllo degli accessi proprie, la cui gestione può essere demandata ad un soggetto diverso dal gestore dell’infrastruttura di virtualizzazione che le ospita. Le *macchini virtuali stabili* sono risorse informatiche dello IIT (come descritto nel paragrafo 2.5), pertanto, per la loro utilizzazione e gestione, dev’essere rispettato quanto stabilito per i dispositivi informatici dell’Istituto.

Non ricadono in questa fattispecie le risorse virtualizzate *effimere*, create per eseguire esperimenti di ricerca di breve o brevissima durata. Tali risorse hanno le seguenti caratteristiche distintive:

- hanno un tempo di vita limitato rispetto alle risorse virtualizzate stabili (tipicamente, vengono create e distrutte all’interno del singolo esperimento, di durata limitata al più a pochi giorni);
- condividono le politiche di accesso delle rispettive macchine fisiche che le ospitano, oppure implementano modelli di accesso estremamente semplici (ad es. singolo utente che può accedere unicamente da macchina che ospita la risorsa virtualizzata);
- non offrono servizi verso Internet.

Vista la loro natura temporanea, tali risorse virtualizzate “effimere” non sono soggette a registrazione nell’archivio delle risorse virtualizzate di cui sopra né al salvataggio dei log di sistema.

4. Incident response

L’incidente è un evento imprevisto, anche accidentale, che causa un’anomalia rispetto al corretto funzionamento di un sistema informatico e può interessare dispositivi, servizi e utenti.

Le segnalazioni degli eventi possono pervenire da utenti, servizi esterni (ad esempio dal CERT nazionale (CSIRT), dal CERT del GARR, ecc.) o da strumenti di monitoraggio automatici. La gestione dell’incidente è coordinata dai *gestori di rete* o dai *gestori dei servizi di Istituto*, i quali analizzano le segnalazioni e, nel caso una di esse venga classificata come incidente, coinvolgono tutti gli utilizzatori ed i gestori della risorsa interessata, al fine di fornire una risposta efficace.

4.1. Processo di gestione dell'incidente

Le fasi di gestione dell'incidente sono le seguenti:

- identificazione e classificazione;
- segnalazione e contenimento;
- bonifica;
- verifica e chiusura.

4.1.1. Identificazione e classificazione

I *gestori di rete* o i *gestori dei servizi di Istituto* stabiliscono se un particolare evento costituisce un incidente correlando informazioni da fonti esterne[8] ed interne[9] all'Istituto. I gestori e gli utilizzatori delle risorse informatiche costituiscono un'ulteriore fonte interna e, a tal proposito, si impegnano a segnalare tempestivamente ogni evento informatico sospetto.
Se viene rilevato un falso allarme il caso si chiude, altrimenti una volta identificato l'incidente, i *gestori di rete* o i *gestori dei servizi* procedono alla classificazione in base all'impatto e al rischio che può costituire per l'Istituto, in accordo con il "*Piano di Gestione del rischio informatico*".

4.1.2. Segnalazione e contenimento

Terminata la fase precedente, si comunica quanto rilevato ai gestori e agli utilizzatori coinvolti, compresi eventuali aspetti tecnici. In accordo con la classificazione dell'incidente, i *gestori di rete* o i *gestori dei servizi di Istituto*, possono intraprendere autonomamente le misure di contenimento ritenute più opportune per limitare potenziali danni all'Istituto. In particolare, tra le misure di contenimento sono previste anche la disconnessione di un dispositivo dalla rete, l'isolamento di una porzione di rete, l'attivazione di protezioni sul firewall di frontiera, il reset della password o la revoca dei permessi in caso di compromissione di un account e analoghi accorgimenti.

4.1.3. Bonifica

È compito dei gestori e degli utilizzatori della risorsa informatica coinvolta nell'incidente intraprendere tutte le azioni necessarie alla bonifica della stessa. In particolare, per le risorse informatiche gravemente compromesse l'azione da intraprendere può consistere nel reinstallare nuovamente il sistema. È compito di gestori ed utilizzatori comunicare ai *gestori di rete o dei servizi* la fine delle attività di bonifica.

[8] GARR-CERT, blacklist, ecc.
[9] Vari strumenti di monitoraggio, firewall, ecc.

4.1.4. Verifica e chiusura

Una volta terminata la fase di bonifica, i *gestori di rete o dei servizi* procedono con la verifica dell'effettiva risoluzione dell'incidente. In particolare, le misure di contenimento adottate vengono gradualmente annullate, verificando l'efficacia delle operazioni di bonifica. In caso positivo, l'incidente viene contrassegnato come chiuso e le restanti misure di contenimento annullate. In caso negativo, si ritorna alla fase di classificazione dell'incidente.

Le comunicazioni avvenute durante tutto il processo vengono archiviate dai *gestori di rete o dei servizi*. In particolare, le procedure e le tecniche apprese durante la gestione di un incidente devono essere utilizzate da tutti i soggetti coinvolti per ridurre la probabilità e l'impatto di eventuali incidenti futuri.

5. Data breach e relativa gestione

La gestione della violazione dei dati personali (Data Breach) è trattata nel documento "*Linee Guida Sulle Procedure di Gestione della Violazione dei Dati Personali (Data Breach)*".

6. Norme di comportamento

Il seguente elenco riporta le principali norme di comportamento relative all'uso delle risorse informatiche, affinché queste siano protette da utilizzi dannosi o illegali, volontari o meno, da parte degli utenti:

- garantire che i dispositivi in uso siano conformi a quanto stabilito nel documento "*Configurazioni standard, minime e sicure dei sistemi operativi*";
- garantire che le credenziali di accesso siano conformi a quanto stabilito nel documento "*Politiche di utilizzo delle credenziali di accesso*";
- custodire adeguatamente le credenziali di accesso ed evitare di fornirle a terzi;
- custodire con le debite cautele i dispositivi in uso;
- bloccare lo schermo o eseguire il logout tutte le volte che si lascia incustodito un dispositivo;
- effettuare sempre il logout da programmi, VPN e piattaforme di lavoro al termine della sessione lavorativa;
- eseguire periodicamente il backup dei dati;
- osservare estrema cautela nell'apertura degli allegati ricevuti via mail da mittenti sconosciuti oppure dei file scaricati da Internet che potrebbero contenere codice malevolo;
- non introdurre consapevolmente software malevolo sulla rete o sui dispositivi dell'Istituto;
- evitare di collegare i dispositivi in uso a reti e VPN sconosciute;

- non utilizzare strumenti o tecniche che possano arrecare danni alle sottoreti o agli utenti dell'Istituto (ad esempio port scanner, security scanner, network monitoring, honeypot, DoS, ecc.);
- non utilizzare access-point Wi-Fi, switch, NAT, o dispositivi analoghi al fine di estendere la connettività di rete, senza il consenso dei gestori di rete e l'autorizzazione del Direttore;
- collaborare con i *gestori di rete* al fine di garantire il corretto funzionamento della stessa;
- non tentare di aggirare i meccanismi di controllo degli accessi di qualsiasi risorsa informatica protetta;
- partecipare ai corsi di formazione inerenti alla security policy organizzati periodicamente dall'Istituto.

Per esigenze particolari non trattate nel precedente elenco fare riferimento al paragrafo *"Policy Compliance"*.

7. Riferimenti e contatti

Sul sito intranet dell'Istituto sono disponibili tutte le informazioni sul Gruppo di Lavoro incaricato per la definizione della policy di sicurezza dello IIT e i contatti dei gestori delle risorse di Istituto a cui fare riferimento.

Tutti i soggetti dovranno prestare attenzione ai messaggi provenienti dalla lista di distribuzione "*security-update@iit.cnr.it*" che conterranno comunicazioni importanti su tutti gli aspetti trattati nella presente policy.

8. Formazione continua del personale

È prevista l'organizzazione periodica di eventi di formazione degli utenti IIT riguardanti il comportamento corretto da osservare durante l'utilizzo della rete, nel rispetto delle norme stabilite dalla presente policy.

Ogni sostanziale modifica del documento sarà accompagnata da un corso di formazione del personale.

9. Validità del documento

L'ultima versione del documento di policy cancella la validità di tutte le versioni precedenti. Il personale dell'Istituto verrà tempestivamente informato ad ogni modifica del documento.

10. Policy Compliance

Eventuali necessità dell'utente non conformi o non previste dalla policy devono essere discusse con il Gruppo di Lavoro incaricato per la definizione della policy di sicurezza dello IIT e, conseguentemente, portate all'attenzione del Direttore.
Eventuali violazioni della policy in oggetto verranno segnalate al Direttore.

11. Riferimenti normativi

Il documento di Policy è scritto in conformità con quanto specificato nelle linee guida AGID per la pubblica amministrazione, con particolare attenzione rivolta alle misure minime (https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict).

12. Lista degli Allegati

I seguenti allegati fanno parte del documento di policy:

- Implementazione Misure di Sicurezza AgID;
- Lista dei software autorizzati;
- Configurazioni standard, minime e sicure dei sistemi operativi;
- Politiche di utilizzo delle credenziali di accesso;
- Piano di Gestione del rischio informatico;
- Linee Guida Sulle Procedure di Gestione della Violazione dei Dati Personali (Data Breach);
- Politiche di utilizzo delle risorse informatiche per il personale non strutturato;
- Richiesta utilizzo apparecchiatura elettronica fuori sede;
- Modulo di accettazione della policy di sicurezza.

Le versioni aggiornate degli allegati sono reperibili sul sito intranet dell'Istituto.

Per una migliore consultazione del technical report gli allegati sopra citati sono stati inclusi nella sezione Appendice.

13. Conclusioni

La normativa italiana impone alle pubbliche amministrazioni l'attuazione di una security policy. Scopo di questo provvedimento, è l'implementazione di procedure per la messa in sicurezza e il corretto utilizzo da parte del personale dell'ente delle risorse informatiche. Un ulteriore elemento significativo è l'adozione di una metodologia per l'individuazione di vulnerabilità e la definizione di protocolli standard da seguire nel caso di avvenuta compromissione di un sistema.

Tutti gli argomenti menzionati sono stati trattati in questo technical report nella descrizione della policy, e sono al momento in fase di implementazione all'Istituto di Informatica e Telematica..

La policy è nella sua prima versione e verrà periodicamente aggiornata per mantenere adeguato il livello di di sicurezza informatica con l'evoluzione delle nuove minacce.

Si ritiene quindi che questo documento possa costituire un punto di riferimento per chi abbia necessità di verificare e/o migliorare la sicurezza della struttura tecnologica della propria Amministrazione.

Appendici

Modello di implementazione misure di sicurezza AGID

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Le risorse attive dell'Istituto sono inventariate in un archivio informatico capace di tener traccia anche del loro MAC Address.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Il software menzionato in ABSC 1.1.1 prevede la possibilità di aggiornare l'inventario via web. È compito di un ufficio preposto aggiornare l'inventario ogni qualvolta un nuovo dispositivo viene approvato.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Si utilizza uno strumento software per correlare temporalmente i MAC Address provenienti dall'inventario delle risorse attive con i rispettivi indirizzi IPv4 e IPv6.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano	

				collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Gli utilizzatori ed i gestori dei dispositivi si assumono la responsabilità di installare ed utilizzare esclusivamente software autorizzato, indicato nel documento "Lista dei software autorizzati".
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Per ogni singolo sistema, è responsabilità di ciascun gestore o utilizzatore assicurarsi che l'elenco del software utilizzato sia nel documento "Lista dei software autorizzati".
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di	

				sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici di inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Fare riferimento al documento "*Configurazioni standard, minime e sicure dei sistemi operativi*" che descrive qualitativamente come eseguire una configurazione standard, minima e sicura. L'utente in grado di effettuare da solo la prima installazione del sistema operativo (*gestore*), deve rispettare quanto previsto da tale documento. Invece, l'utente non in grado di effettuare da solo la prima installazione del sistema operativo (*utilizzatore*), è supportato da un apposito ufficio che la esegue in sua vece, applicando una configurazione sicura prevista dal documento menzionato precedentemente. In entrambi i casi, alla fine della procedura, l'eventuale software installato deve essere compreso nella lista del software autorizzato, come indicato in ABSC 2.1.1.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini di installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Fare riferimento al documento "*Configurazioni standard, minime e sicure dei sistemi operativi*".

3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Esistono diversi livelli di compromissione, compresi tra un livello di compromissione minima (non grave), fino ad un livello di compromissione massima (molto grave): ● in caso di una compromissione ***non grave***, si procede al ripristino della configurazione standard semplicemente utilizzando un programma antivirus/antimalware sul sistema compromesso; ● in caso di compromissione ***molto grave*** per ripristinare la configurazione standard si procede con la disconnessione del sistema dalla rete, la formattazione del disco ed applicando quanto riportato in ABSC 3.1.1; ● in casi di compromissione compresi tra il livello minimo ed il livello massimo, occorre gestire il ripristino caso per caso.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Per i prodotti che lo prevedono, si utilizzano supporti di memorizzazione (memorie USB, CD/DVD, ecc.) contenenti le immagini di installazione dei sistemi operativi utilizzati in Istituto. La gestione di questi supporti è demandata a un apposito ufficio.
3	3	2	S	Le immagini di installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	L’amministrazione remota degli host avviene solamente tramite protocolli intrinsecamente sicuri.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque	

				alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Si utilizzano strumenti di Vulnerability Assessment che sulla base di scansioni periodiche producono report con indicazioni sulla criticità delle vulnerabilità scoperte.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	

4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	I sistemi di Vulnerability Assessment discussi nello ABSC 4.1.1, prevedono funzionalità di aggiornamento automatico.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'installazione delle patch e degli aggiornamenti del software viene effettuata tenendo conto della tipologia del sistema: ● per i server che ospitano servizi critici, sono utilizzate le funzionalità messe a disposizione dal sistema operativo per l'installazione manuale degli aggiornamenti, poiché occorre valutare caso per caso se è opportuno applicare l'aggiornamento al fine di non arrecare disservizi; ● per tutti gli altri sistemi sono utilizzate le funzionalità di aggiornamento automatico messe a disposizione dal sistema operativo e dalle applicazioni. Nel caso di esigenze particolari, è possibile installare manualmente gli aggiornamenti e limitare l'installazione automatica a quelli riguardanti la sicurezza.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Si utilizzano procedure off-line mediante supporti rimovibili, come indicato dal produttore del sistema air-gapped.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi	

				privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	La risoluzione delle vulnerabilità viene verificata confrontando l'ultimo report prodotto dagli strumenti di Vulnerability Assessment con quello precedente.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Fare riferimento al documento *"Piano di gestione del rischio informatico"*.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Fare riferimento al documento *"Piano di gestione del rischio informatico"*.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Sono definite le seguenti classi di utenti: ● **gestori:** utenti che gestiscono in autonomia il proprio dispositivo (laptop/workstation). Questa tipologia di utenti dispone di credenziali di accesso che consentono il massimo livello di privilegi. Pertanto, un utente appartenente a questa tipologia, si assume la piena responsabilità

					di gestione del proprio dispositivo; ● **utilizzatori:** utenti che demandano la gestione del proprio dispositivo (laptop/workstation) ad un ufficio preposto. Questa tipologia di utenti dispone di credenziali di accesso che consentono un livello di privilegi limitato.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	I gestori devono operare con privilegi di amministratore solo nei casi necessari. La registrazione degli accessi effettuati è demandata al sistema operativo.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I nomi utente delle utenze amministrative autorizzate, compresi quelli di sistemi virtuali, sono inventariati utilizzando un archivio informatico protetto.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Viene adottata una politica di cambio delle credenziali di default per tutti i nuovi dispositivi collegati alla rete. Le nuove credenziali immesse, devono essere conformi al documento denominato *"Politiche di utilizzo delle credenziali di accesso"*.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta una utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password	

				(OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Gli utenti devono scegliere le proprie password in accordo con quanto previsto dal documento denominato *"Politiche di utilizzo delle credenziali di accesso"*.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La periodicità di sostituzione e/o aggiornamento delle password è stabilita nel documento denominato "Politiche di utilizzo delle credenziali di accesso".
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Laddove previsto, il riutilizzo delle password a breve distanza di tempo viene impedito tramite meccanismi automatici del sistema. Negli altri casi, gli utenti si assumono la responsabilità di non riutilizzare le password già usate in precedenza.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Per quanto riguarda l'utilizzo ordinario del proprio dispositivo, ciascun utente deve utilizzare utenze non privilegiate. L'uso di un'utenza privilegiata dev'essere limitata ai soli casi strettamente necessari. In alternativa, si può considerare, partendo da un'utenza non privilegiata, di elevare i propri privilegi a utenza privilegiata.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Far riferimento al documento "Politiche di utilizzo delle credenziali di accesso".
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per	Far riferimento al documento "Politiche di utilizzo delle credenziali di accesso".

				le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative anonime dei server istituzionali, dei laptop e/o delle workstation gestite da un apposito ufficio sono conservate in busta chiusa ed in un luogo sicuro, sotto la responsabilità del Direttore. Inoltre, per tutte le utenze amministrative (anonime e non) è ammesso l'uso di software di tipo "password manager" esclusivamente su infrastruttura d'Istituto.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Far riferimento al documento "Politiche di utilizzo delle credenziali di accesso".

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Ove possibile, è obbligatoria l'installazione di un sistema antivirus su tutti i dispositivi laptop e workstation. Per quanto riguarda i sistemi Linux e Mac, dev'essere almeno installato il tool *chrootkit* per rilevare la presenza di rootkit nel sistema scansionato. L'elenco degli antivirus consentiti è riportato nel documento "Lista dei software autorizzati".
8	1	2	M	Installare su tutti i dispositivi firewall e IPS personali.	Ove possibile, è obbligatoria l'installazione di firewall e IPS sui dispositivi personali. Sui server istituzionali è compito del gestore valutare se sia opportuno usare una soluzione firewall e IPS. L'elenco di firewall e IPS consentiti è riportato nel documento "Lista dei software autorizzati".

8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	È responsabilità di ciascun utente utilizzare solo dispositivi esterni strettamente necessari per le attività lavorative (ad es. laptop personali, memorie USB, ecc.).
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimovibili.	È responsabilità di ciascun gestore di un dispositivo assicurarsi che siano state disattivate: ● l'esecuzione automatica dei contenuti provenienti da supporti rimovibili, ● l'esecuzione automatica delle macro,
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	

8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	● l'apertura automatica dei messaggi di posta elettronica, ● l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	È responsabilità di ciascun utente abilitare la funzionalità di scansione automatica dell'antivirus, anche per i supporti rimovibili al momento della loro connessione.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Filtri antispam sono attivi sul server di posta d'istituto.
8	9	2	M	Filtrare il contenuto del traffico web.	Al fine di rilevare la presenza di malware, spyware e/o vulnerabilità note, il traffico di rete non cifrato è ispezionato automaticamente dal firewall di frontiera.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Sono utilizzati gli stessi strumenti descritti negli ABSC 8.9.1 e ABSC 8.9.2.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	L'istituto utilizza un sistema di backup centralizzato. A discrezione del gestore, i server utilizzano tale sistema, o in alternativa un sistema di backup specifico per ciascun servizio approvato dal Direttore. Le workstation e i laptop utilizzano il sistema centralizzato di Istituto oppure dispositivi di backup individuali. Tutti i backup sono effettuati con frequenza almeno settimanale.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Occorre fare una distinzione tra backup ordinario e backup di sicurezza: ● il **backup ordinario** è tipicamente eseguito per garantire il corretto funzionamento di un servizio, pertanto esso può essere conservato, senza l'utilizzo di meccanismi di cifratura, all'interno del sistema su cui è stato eseguito (ad es. su una partizione disco differente da quella che contiene il sistema operativo e tutto il software utilizzato); ● il **backup di sicurezza**, invece, deve avvenire, in accordo con quanto specificato nell'ABSC 10.1.1, su un sistema fisicamente separato da quello per cui esso viene effettuato. Se non adeguatamente protetto fisicamente (ad es. scollegato dalla rete e ben custodito), tale sistema deve disporre di un meccanismo di cifratura dei dati.

10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	È responsabilità del gestore garantire che almeno una copia di sicurezza sia conservata su un sistema fisicamente separato. Tale sistema deve essere adeguatamente protetto. In alternativa, le copie di sicurezza in esso memorizzate devono essere cifrate. Inoltre, il gestore del sistema garantisce che almeno una copia non sia permanentemente accessibile.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Ove possibile, la riservatezza di alcuni dati presenti sui server istituzionali deve essere garantita (ad es. dati sensibili all'interno di database o LDAP, ecc.). I dati con particolari requisiti di riservatezza (dati rilevanti) sono protetti mediante meccanismi di cifratura o altrimenti con altre politiche di sicurezza adeguate alla loro protezione.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle	

				workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Sul firewall di frontiera è applicato un filtraggio basato su blacklist aggiornate dinamicamente e contenenti indirizzi IP e URL che si riferiscono a host e siti malevoli.
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

Lista dei software autorizzati

Il seguente documento contiene la lista delle risorse software, divise per categorie, che possono essere utilizzate nei dispositivi d'Istituto. La loro politica di utilizzo è descritta nella policy di sicurezza informatica dello IIT alla sezione *"Uso del software"*.

Questa lista viene costantemente aggiornata in accordo con le esigenze di utilizzo e sicurezza informatica dell'Istituto. Di conseguenza, sarà possibile che alcune risorse software vengano aggiunte, mentre altre vengano eliminate in quanto obsolete, non più supportate oppure ritenute inadeguate dal punto di vista della sicurezza.

La lista non indica le versioni software, di conseguenza i software utilizzabili sono esclusivamente quelli per cui vengono ancora rilasciati aggiornamenti di sicurezza e mantenuti dal produttore.

In questa prima versione la lista non è completa, di conseguenza la sua espansione e l'armonizzazione delle attuali risorse software utilizzate in Istituto saranno affrontate nelle prossime release del documento di policy.

Sistemi operativi

- Windows desktop/server
- Mac OS desktop/server
- OS basati su GNU Linux desktop/server

Tutti i software contenuti all'interno delle distribuzioni dei sistemi operativi o repository/store ufficiali sono considerati autorizzati, nel rispetto della policy di sicurezza di Istituto.

Sicurezza

- F-Secure Client Security
- SentinelOne Endpoint Protection
- Windows Defender / Windows Firewall

Ufficio

- Adobe Acrobat Reader
- Adobe Acrobat Professional
- Adobe Creative Suite
- suite LibreOffice
- suite Microsoft Office
- suite OpenOffice
- TexMaker

File sharing/transfer

- Dropbox

- Google Drive
- Microsoft OneDrive
- Seafile

Instant messaging/collaboration

- GoToMeeting
- Skype
- Telegram
- Vidyo
- Whatsapp
- Zoom

Web Browser

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Opera
- Safari

Multimedia

- VLC media player

Utility

- WinRar
- Toast Titanium
- Nero burning room suite
- PlayonMac
- Intermapper
- Filezilla
- Cool term
- Z term
- Wireshark
- Inkscape
- Paintbrush
- Mendeley desktop

Posta elettronica

- Mozilla Thunderbird

Virtualizzazione

- Oracle VirtualBox

- VMWare workstation player

Sviluppo

- Eclipse
- Netbeans
- Anjuta
- Sublime
- Mysql benchmark

Password Manager

- Passbolt
- Keepass

Backup

- Acronis Backup

Configurazioni standard, minime e sicure dei sistemi operativi

Il presente documento contiene le linee guida da seguire per la prima installazione e l'utilizzo nel tempo dei principali dispositivi connessi alle sottoreti di Istituto.

Prima di procedere con la configurazione del sistema operativo, assicurarsi che il dispositivo da configurare sia stato collaudato e inventariato.
Tutti i dispositivi personali non di proprietà dello IIT, devono essere autorizzati dal direttore prima di essere connessi alle reti d'istituto. Anche in questo caso, il soggetto si impegna a rispettare quanto stabilito dalla policy d'Istituto.

Workstation/Laptop

Di seguito sono riportate le principali fasi e operazioni da eseguire per installare e configurare un dispositivo appartenente alla categoria "Workstation/Laptop":

- utilizzare una procedura di installazione ufficiale del sistema operativo. Nel caso in cui il sistema operativo richieda una licenza d'uso, questa dev'essere ottenuta attraverso canali ufficiali (ad esempio: rivenditore, apposito ufficio, ecc.);
- utilizzare esclusivamente i sistemi operativi elencati nel documento *"Lista dei software autorizzati"*;
- configurare il sistema operativo in modo tale da poter essere connesso alla rete di Istituto;
- per la gestione degli account, rispettare quanto stabilito nel documento *"Politiche di utilizzo delle credenziali di accesso"*;
- creare esclusivamente l'account utente relativo alla persona che utilizzerà il sistema: se la persona in oggetto gestisce autonomamente il dispositivo, avrà un account con ruolo di amministratore. In caso contrario, il dispositivo sarà gestito dall'ufficio preposto tramite un account di amministrazione, mentre l'utente avrà un account con privilegi limitati.
- eliminare/disabilitare eventuali account presenti e non utili ai fini del funzionamento del sistema (ad esempio "guest");
- installare un software antivirus e un firewall scelti tra quelli elencati nel documento *"Lista dei software autorizzati"*;
- abilitare la funzionalità di scansione automatica dell'antivirus, anche per i supporti rimovibili al momento della loro connessione;
- impostare il download e l'installazione automatica degli aggiornamenti di sicurezza e critici di sistema;
- mantenere aggiornati il sistema operativo e le applicazioni in uso, ove possibile;
- installare esclusivamente software autorizzato, indicato nel documento *"Lista dei software autorizzati"*;
- attivare la procedura di backup dei dati con frequenza almeno settimanale utilizzando le funzionalità offerte dal sistema operativo e/o tramite un

software apposito presente nella “Lista dei software autorizzati”. L’archiviazione può avvenire su un dispositivo di storage personale o sul sistema di Istituto. In caso di dati sensibili, assicurarsi di proteggere le copie di backup utilizzando opportune procedure crittografiche;
- abilitare il blocco schermo, protetto da password, che entri in funzione automaticamente dopo un’inattività massima di dieci minuti;
- disattivare l’esecuzione automatica dei contenuti provenienti da supporti rimovibili;
- disattivare l’esecuzione automatica delle macro, a meno che l’attività che l’utilizzatore svolge non lo richieda;
- disattivare l’apertura automatica dei messaggi di posta elettronica;
- disattivare l’anteprima automatica dei contenuti dei files.

Server

Di seguito sono riportate le principali fasi e operazioni da eseguire per installare e configurare un dispositivo appartenente alla categoria “Server”:

- utilizzare le versioni di sistema operativo esclusivamente elencate nel documento “Lista dei software autorizzati”;
- utilizzare una procedura di installazione ufficiale del sistema operativo. Nel caso in cui il sistema operativo richieda una licenza d’uso, questa dev’essere ottenuta attraverso canali ufficiali (ad esempio: rivenditore, apposito ufficio, ecc.);
- configurare il sistema operativo in modo tale da poter essere connesso alla sottorete dei servizi istituzionali o a quella per ricerca e sviluppo di Istituto;
- per la gestione degli account, rispettare quanto stabilito nel documento *“Politiche di utilizzo delle credenziali di accesso”*;
- installare un software antivirus e un firewall scelti tra quelli elencati nel documento *“Lista dei software autorizzati”*;
- disabilitare l’accesso remoto SSH per l’utente root. Se indispensabile, abilitarlo attraverso chiave pubblica/privata, evitando l’utilizzo di password e restringendo l’accesso ai soli IP remoti strettamente necessari al sistema;
- abilitare o disabilitare gli aggiornamenti automatici in relazione alle esigenze dei servizi ospitati sul server. Nel caso in cui gli aggiornamenti automatici siano stati disabilitati dal gestore, è necessario abilitare la loro notifica automatica;
- attivare solo i servizi prettamente necessari, disabilitando tutti i servizi non utilizzati;
- installare esclusivamente software autorizzato, indicato nel documento *“Lista dei software autorizzati”*;
- predisporre delle funzionalità di backup, in modo da recuperare la piena operatività del sistema in caso di guasti o malfunzionamenti. Nel caso che il sistema utilizzi dati sensibili, assicurarsi di proteggere i backup utilizzando opportune procedure crittografiche.

Stampanti di rete

Di seguito sono riportate le principali operazioni da eseguire per installare e configurare un dispositivo appartenente alla categoria “Stampanti di rete”:

- verificare che la versione del firmware installato sia quella consigliata dal produttore;
- configurare il dispositivo in modo tale da poter essere connesso alla rete “utenti di Istituto”;
- per quanto riguarda le utenze amministrative, rispettare quanto stabilito nel documento *“Politiche di utilizzo delle credenziali di accesso”*;
- se possibile, abilitare il protocollo HTTPS per l’interfaccia di gestione web;
- disabilitare le funzionalità avanzate non necessarie e/o non utilizzate;
- disabilitare i canali di accesso alla stampante (ad esempio Wi-Fi, bluetooth, ecc.) non necessari e/o non utilizzati;
- ottenere un indirizzo IP per la stampante dall’ufficio preposto all’assegnazione degli indirizzi;
- comunicare l’indirizzo IP della stampante ai gestori di rete per la sua protezione sul firewall perimetrale.

Network Attached Storage (NAS)

Di seguito sono riportate le principali operazioni da eseguire per installare e configurare un dispositivo appartenente alla categoria NAS:

- verificare che la versione del firmware installato sia quella consigliata dal produttore;
- configurare il dispositivo in modo tale da poter essere connesso alla rete “utenti di Istituto”;
- per quanto riguarda le utenze, rispettare quanto stabilito nel documento *“Politiche di utilizzo delle credenziali di accesso”*;
- se possibile, abilitare esclusivamente protocolli intrinsecamente sicuri per la gestione del dispositivo;
- assicurarsi che siano abilitate esclusivamente le funzionalità per consentire il backup dei dati da altri dispositivi o l’espansione dello spazio disco;
- disabilitare le funzionalità avanzate non necessarie e/o non utilizzate;
- ottenere un indirizzo IP per il NAS dall’ufficio preposto all’assegnazione degli indirizzi;
- comunicare l’indirizzo IP del dispositivo ai gestori di rete per la protezione su firewall perimetrale.

Altri dispositivi

Qualora un dispositivo non appartenga a nessuna delle categorie precedentemente elencate, è necessario rivolgersi ai gestori di rete e dei servizi d’Istituto per definirne la procedura ottimale di installazione e protezione.

Politiche di utilizzo delle credenziali di accesso

Obiettivi generali

Il presente documento ha lo scopo di definire le procedure per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali usate per accedere alle risorse informatiche protette dell'Istituto ed è rivolto a tutto il personale dello IIT. Le procedure in esso contenute si riferiscono principalmente alla modalità di accesso basata su *username e password*, la quale rappresenta la modalità di accesso alle risorse di Istituto più usata. Altre procedure definite per modalità di accesso meno comuni (ad esempio autenticazione basata su chiavi pubbliche) sono riportate alla fine del documento.

Termini e definizioni

Coerentemente con quanto definito nella security policy d'Istituto, si definiscono risorse informatiche dell'istituto: l'infrastruttura di rete, i dati sensibili, i servizi informatici, il software ed i dispositivi informatici in uso all'interno dell'Istituto. Inoltre, con il termine risorsa informatica protetta si intende una risorsa informatica che, tramite un meccanismo di controllo degli accessi, è disponibile solamente ai soggetti autorizzati.

In aggiunta, il personale dello IIT coinvolto nell'uso e nella gestione di risorse informatiche può ricoprire vari ruoli: utilizzatore, gestore, *gestore di rete* e *gestore dei servizi*.
Per semplicità di trattazione all'interno del presente documento, quando non diversamente specificato, il termine "*gestore*" è usato per rivolgersi ai ruoli di *gestore*, *gestore di rete* e *gestore dei servizi*, mentre il termine *"soggetto"* è usato per rivolgersi a tutti i ruoli.

Per maggiori dettagli consultare i paragrafi *"Risorse informatiche dell'Istituto"* e *"Accesso a risorse protette"* della security policy d'Istituto.

Norme generali

Di seguito sono riportate le norme generali da osservare per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali:

- le credenziali di accesso sono strettamente personali ed è responsabilità di ciascun soggetto custodirle in modo adeguato. Per questo motivo, non è consentito condividerle con soggetti terzi;
- ove possibile, è responsabilità del gestore modificare le credenziali del *superutente predefinito*[10]. Inoltre, il superutente non deve essere utilizzato normalmente, né per le operazioni ordinarie né per le operazioni di

[10] l'utente con privilegi massimi il cui username è predefinito dal sistema utilizzato (ad es. root, Administrator, admin, ecc.)

gestione del sistema;

- nel caso in cui un soggetto sospetti un utilizzo non autorizzato delle proprie credenziali, è sua responsabilità segnalare tempestivamente l'eventualità al gestore del sistema coinvolto o ad un suo delegato. Sarà cura del soggetto stesso impostare una nuova password associata al proprio account o chiedere al gestore del sistema di impostarne una nuova per suo conto;
- è responsabilità dell'utilizzatore modificare la password assegnata da un gestore o da un suo delegato al primo accesso al sistema o nel caso di ripristino della password (vedi punto precedente);
- la password di accesso ha validità massima di 6 mesi, pertanto è responsabilità dell'utilizzatore modificarla entro tale scadenza pena la perdita di validità e conseguente sospensione dell'account. Nei sistemi che lo prevedono, se l'account viene sospeso a causa della scadenza temporale della password, l'utilizzatore può provvedere a riabilitarlo configurando una nuova password;
- è responsabilità di ciascun soggetto rispettare i seguenti criteri per la creazione di una password robusta:
    - lunghezza di almeno 8 caratteri;
    - contenere caratteri in maiuscolo e minuscolo, numeri e caratteri speciali (simboli);
    - non contenere caratteri accentati e spazi.

Di seguito sono riportate alcune raccomandazioni relative alla creazione, all'utilizzo, alla conservazione ed alla gestione delle credenziali:

- non utilizzare le password usate per l'accesso ai servizi istituzionali su servizi di terze parti;
- non salvare le password in chiaro su file non protetti sul proprio computer, su supporti rimovibili o su sistemi di condivisione file;
- non trascrivere le password in qualsiasi luogo non adeguatamente custodito;
- non costruire la password utilizzando informazioni personali (ad esempio nome, cognome, data di nascita, targa veicolo, ecc.);
- non utilizzare parole comuni;
- non riutilizzare le stesse password. Ad ogni cambio delle credenziali impostarne una nuova.

Inoltre, si raccomanda di:

- prestare la massima attenzione quando si forniscono credenziali di accesso a servizi Internet non istituzionali;
- evitare di fornire credenziali di accesso a richieste pervenute via email, poiché in nessun caso un gestore o un suo delegato richiederanno ad un soggetto di comunicare le proprie credenziali via email.

Si noti infine che è possibile utilizzare applicazioni “password manager”, per gestire e memorizzare le proprie credenziali, purché rispettino adeguati standard di sicurezza. A questo scopo, è cura del soggetto fare riferimento al documento *“Lista dei software autorizzati”*.

Gestori dei servizi

Per garantire disponibilità e riservatezza, le credenziali relative ad utenze amministrative anonime (ad esempio root o Administrator) dei sistemi su cui sono ospitati servizi istituzionali e apparati di rete devono essere conservate presso un ufficio preposto designato dal direttore d’Istituto. Non devono essere utilizzate per le operazioni ordinarie o di gestione del sistema, ma solo in caso di comprovata e giustificata necessità approvata dal Direttore (ad esempio nel caso in cui i gestori preposti siano irreperibili). Anche questo tipo di credenziali è soggetto a quanto definito nel paragrafo “Norme generali” ad eccezione dei seguenti casi:

- il periodo di validità può essere più lungo di 6 mesi (fino ad un massimo di 2 anni);
- la lunghezza della password deve essere almeno di 14 caratteri.

Compatibilmente con il funzionamento del sistema/apparato di rete, ove possibile è responsabilità del gestore implementare quanto segue:

- un meccanismo che impedisca l’accesso agli utilizzatori con password non aggiornata da più di 6 mesi;
- una procedura sicura che consenta autonomamente all’utilizzatore di modificare o reimpostare una nuova password.

Al fine di garantire l’univocità e la storicizzazione delle attività informatiche, ove possibile è responsabilità del gestore impedire il riutilizzo di username scelti precedentemente.

Gli archivi informatici (log) devono essere conservati nei modi e termini temporali previsti dalle normative vigenti.

Le credenziali non devono permettere un privilegio di accesso superiore a quello richiesto per operare e devono essere disattivate nel momento in cui l’utilizzatore non ha più diritto ad utilizzare la risorsa protetta.

I sistemi che memorizzano credenziali di accesso devono prevedere meccanismi di hashing non deprecati, in modo che le password siano difficilmente decifrabili, anche in caso di data breach.

Si deve evitare che le password in chiaro compaiano nei file di log e durante le operazioni di debug e troubleshooting dei sistemi.

Si raccomanda di implementare sistemi di avviso che segnalino un utilizzo anomalo delle credenziali, come ad esempio accessi ripetuti da aree geografiche distanti, tentativi di brute-force, ecc. Nel caso in cui venga rilevata un'attività sospetta il gestore può disabilitare temporaneamente un account, segnalandolo al soggetto coinvolto.

Credenziali per terze parti

Per un periodo strettamente necessario ed in contesti ben circoscritti (ad esempio, partner di progetti di ricerca, supporto tecnico remoto, ecc.), un gestore, previa autorizzazione del Direttore, può concedere a terze parti l'accesso ad una risorsa di Istituto.

Le credenziali rilasciate devono rispettare quanto indicato nel paragrafo "*Norme generali*" per quanto concerne la loro gestione e il loro utilizzo. Dovranno inoltre essere riconducibili all'utilizzatore e all'attività e godere del livello di privilegio appropriato alle operazioni da svolgere.

Al termine del suddetto periodo di attività, tali credenziali dovranno essere disabilitate.

Gestori di dispositivi (laptop, workstation, stampanti e NAS)

La password di accesso al sistema deve essere modificata ogni 6 mesi. È responsabilità del gestore provvedere a tale operazione. Si richiama la sezione "*Norme generali*" per il corretto comportamento da adottare.

Credenziali di autenticazione alternative

In questo paragrafo si fa riferimento a procedure di autenticazione non basate sull'utilizzo di username e password.

Autenticazione con chiavi crittografiche

Per facilitare la gestione di risorse protette tramite il protocollo SSH, è consentito utilizzare le chiavi crittografiche come meccanismo di autenticazione alternativo a username e password.

Ogni coppia di chiavi SSH include una chiave *pubblica* che viene copiata sui server e una *privata* che resta all'utente. Poiché quest'ultima consente l'accesso al sistema remoto deve essere archiviata e gestita con particolare cura.

Si raccomanda di utilizzare chiavi RSA ad almeno 2048 bit (o preferibilmente a 4096 bit) e se possibile proteggere la chiave privata tramite passphrase.

L'autenticazione mediante chiavi SSH equivale ad un accesso basato su username e password; pertanto chi ne fa uso deve prestare massima attenzione alla riservatezza delle chiavi.

Altri meccanismi di autenticazione

Per i dispositivi personali (ad esempio gli smartphone o laptop muniti di lettore di impronte digitali) è concesso l'uso di fattori biometrici al fine di ottenere l'autenticazione sul dispositivo.
Altre metodologie di autenticazione dovranno essere preventivamente approvate dal Direttore.

Piano di Gestione del rischio informatico

Questo argomento sarà trattato nelle prossime release della policy.

Linee Guida Sulle Procedure di Gestione della Violazione dei Dati Personali (Data Breach)

Documento non incluso nel Rapporto Tecnico.

Politiche di utilizzo delle risorse informatiche per il personale non strutturato

Documento non incluso nel Rapporto Tecnico.

Richiesta utilizzo apparecchiatura elettronica fuori sede

Documento non incluso nel Rapporto Tecnico.

Modulo di accettazione della policy di sicurezza

Documento non incluso nel Rapporto Tecnico.