PROVINCIA DI PISA

**Istituzione dei Comuni per il governo dell'area vasta**
**Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente**
**Gestione associata di servizi e assistenza ai Comuni**

# DECRETO DEL PRESIDENTE

Decreto nr. 126 del 31/12/2024

**Oggetto:** DISCIPLINARE INERENTE LE MISURE DI SICUREZZA INFORMATICA DA ADOTTARE SULLE POSTAZIONI DI LAVORO

**Hash:**

DEL_DECP_126_2024.pdf.p7m
C6CDA16EB75F3D1D45015BDCB293303715A0051246B07ED17A268D855453EF1DC22D52D
357774F684E1B0E14F870BD66690950508CA4188C6A29BBE1D056ECC5

Disciplinare sicurezza informatica.pdf.p7m
43545115245EBD8AE46096038BA944801AC7EC38B7AB3EF26F079C20D5EA8039A1430AA
DDA519D009D27B5B9F1AF85C93E4303D17661B600AF8961BF914AD5EF

PROVINCIA DI PISA

**Istituzione dei Comuni per il governo dell'area vasta**
**Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente**
**Gestione associata di servizi e assistenza ai Comuni**

SETTORE AFFARI E SERVIZI GENERALI. SERVIZI AMBIENTALI E TERRITORIALI.

# DECRETO PRESIDENZIALE

Proposta nr. 3753 del 2024
Decreto nr. 126/2024

**Oggetto:** DISCIPLINARE INERENTE LE MISURE DI SICUREZZA INFORMATICA DA ADOTTARE SULLE POSTAZIONI DI LAVORO

## IL PRESIDENTE

Nell'esercizio dei poteri assunti ai sensi e per gli effetti del D.Lgs. 267/2000 Testo Unico degli Enti Locali e della Legge 56/2014;

Con l'assistenza del Segretario generale ai sensi e per gli effetti dell'art. 97, comma 2, T.U. n° 267/2000, in ordine alla conformità dell'azione amministrativa alle leggi, allo statuto ed ai regolamenti;

RICHIAMATI

- il Codice dell'Amministrazione Digitale (CAD) - D.Lgs. 7 marzo 2005, n. 82, che stabilisce i principi per l'organizzazione digitale della Pubblica Amministrazione, includendo la sicurezza delle informazioni e dei sistemi digitali (articoli 50-bis e seguenti);
- il Regolamento UE n. 679/2016: Regolamento generale sulla protezione dei dati (GRPR);
- il Decreto Legislativo 30 giugno 2003, n. 196, modificato dal D.Lgs. 10 agosto 2018, n. 101 "*Codice in materia di protezione dei dati personali*" che adegua la normativa italiana al GDPR stabilendo le regole sulla protezione dei dati personali, comprese misure tecniche e organizzative per la sicurezza dei dati;
- il Piano Triennale per l'Informatica nella Pubblica Amministrazione che definisce linee guida e strategie per la trasformazione digitale e la sicurezza ICT nella PA;
- la Circolare n. 2 del 18 aprile 2017 dell'Agenzia per l'Italia Digitale recante le misure minime di sicurezza che debbono essere adottate per contrastare le minacce più comuni e frequenti per i sistemi informativi della PA;
- il Decreto Legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133 "*Norme relative alla sicurezza cibernetica nazionale*" che richiede alle PA di garantire standard elevati di protezione informatica;
- il Framework nazionale per la Cybersecurity sviluppato dal Consorzio Interuniversitario Nazionale per l'Informatica per la gestione del rischio informatico in linea con gli standard internazionali;

- il D.lgs. n. 138/2024 di recepimento della direttiva UE 2022/2555, che stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale;

SENTITO il Responsabile per la Transizione al Digitale, dr. Paola Fioravanti, incaricato con DP n. 39/2023, nel suo ruolo di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture informatiche dell'ente;

RITENUTO OPPORTUNO accompagnare tale servizio da un'opportuna regolamentazione che ne disciplini l'utilizzo;

VISTA la proposta di "Disciplinare inerente le misure di sicurezza informatica da adottare sulle postazioni di lavoro" (allegato A), ritenuta meritevole di approvazione;

VISTO il parere favorevole di regolarità tecnica espresso dal Dirigente del Settore Affari e Servizi Generali, Servizi Ambientali e Territoriali e omesso il parere di regolarità contabile tenuto conto che l'atto non comporta riflessi diretti sulla situazione economico-finanziaria e/o sul patrimonio dell'Ente, ai sensi dell'art. 49, comma 1, del D. Lgs 267/2000 e ss.mm.ii.

ACCERTATA la propria competenza alla emanazione del presente atto ai sensi dell'art. 50 del D.Lgs. n. 267/2000, Testo Unico degli Enti Locali e della Legge 56/2014 cd Delrio;

**DECRETA**

Per i motivi espressi in premessa che si richiamano integralmente:

1 Di approvare il "Disciplinare inerente le misure di sicurezza informatica da adottare sulle postazioni di lavoro" allegato A del presente atto, del quale costituisce parte integrante e sostanziale.

2 Di dichiarare che il presente disciplinare sarà aggiornato per recepire le disposizioni derivanti dall'approvazione di nuove norme e regolamenti relativi alla tutela della privacy, alla protezione dei dati, all'uso dei servizi informatici e telematici;

3 Di disporre la pubblicazione del disciplinare sul sito web istituzionale e sulla intranet dell'Ente;

4 Di demandare agli uffici competenti della Provincia l'attivazione di tutte le azioni necessarie all'attuazione ed al rispetto del disciplinare;

5 Di dichiarare il presente provvedimento immediatamente eseguibile, stante l'esigenza di introdurre con la massima tempestività le necessarie misure di contrasto ai rischi per la sicurezza informatica della provincia tramite gli interventi di cui trattasi.

**Approvato e sottoscritto con firma digitale:**
**Il Presidente**
Massimiliano Angori

**ALLEGATO A**

PROVINCIA DI PISA
UO Tecnologie Informatiche, Fonia e Innovazione

# Disciplinare inerente le misure di sicurezza informatica da adottare sulle postazioni di lavoro

## 1) Introduzione

Con la Circolare n. 2 del 18 aprile 2017, l'Agenzia per l'Italia Digitale ha definito l'elenco delle "*Misure minime per la sicurezza ICT delle pubbliche amministrazioni*" che debbono essere adottate per contrastare le minacce più comuni e frequenti per i sistemi informativi della PA. Tali misure di sicurezza informatica si articolano su tre livelli di cui un livello "minimo" al quale ogni pubblica amministrazione deve necessariamente essere conforme, e due livelli successivi che rappresentano situazioni più evolute.

Per garantire la sicurezza dei sistemi informatici su tutte le postazioni di lavoro collegata alla rete dell'ente devono essere adottate le suddette misure minime con le modalità descritte in questo documento.

In particolare:

- tutti gli utenti sono invitati a leggere e seguire quanto indicato nel paragrafo 2 ("*Raccomandazioni di Sicurezza Valide per tutti gli Utenti*");
- gli utenti in possesso di credenziali con diritti amministrativi, e che pertanto sono in grado di operare in qualità di "*amministratori di sistema*" sui dispositivi gestiti, devono seguire le ulteriori indicazioni del paragrafo 3 "*Raccomandazioni di Sicurezza Valide per gli Amministratori di Sistema*".

## Glossario

- Amministratore di Sistema: utente che, essendo dotato di privilegi di amministratore di macchina, può modificare la configurazione del sistema operativo e dei software installati su un sistema di elaborazione;
- Endpoint: in questo contesto si intende la singola postazione di lavoro desktop o notebook (alias PC)
- Agente di Sicurezza Endpoint: software di sicurezza (attualmente BitDefender Gravity Zone), da installare su tutte le postazioni di lavoro, che integra funzioni di antivirus e antimalware, endpoint detection & response (EDR), protezione avanzata dalle minacce e gestione del rischio.
- Agente di gestione Endpoint: software di gestione (attualmente Ninja RMM) , da installare su tutte le postazioni di lavoro, che effettua l'inventario hardware e software, gli aggiornamenti del sistema operativo e delle applicazioni, il backup della postazione di lavoro e permette una gestione remota dai dispositivi da parte degli amministratori di sistema.

## 2) Raccomandazioni di Sicurezza Valide per tutti gli Utenti

Le raccomandazioni di seguito valgono per tutti gli utenti che utilizzano dispositivi collegati alla rete della Provincia di Pisa.

a) Per tutte le utenze di dominio (normalmente utilizzate per accedere al Pc, alla posta elettronica, alle condivisioni di rete ed ai programmi Sfera e Prisma) esiste una "*policy*" automatica che ne verifica la complessità e forza la modifica ogni 90 giorni. In tutti gli altri casi è necessario impostare password con lunghezza di almeno 8 caratteri, con combinazioni di lettere, numeri e caratteri speciali, e modificarle almeno ogni 90 giorni.

b) Conservare tutte le proprie password in modalità sicura e protetta, non scriverle su fogli o post-it, non comunicarle a voce o via email ad alcuno.

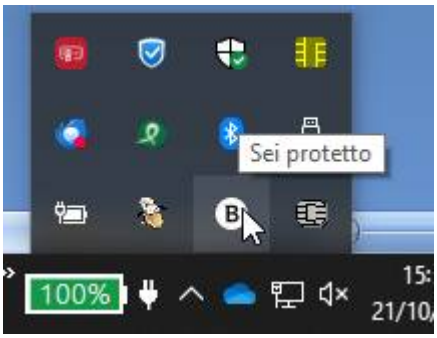
c) Cambiare immediatamente una password che è stata per qualche motivo comunicata a terzi o che si sospetti abbia perso il requisito di segretezza.

d) Evitare di salvare le password sul browser ma digitarla sempre ad ogni nuovo accesso.

e) Impostare sempre uno screen-saver con richiesta di password o altro meccanismo di sicurezza (es. utilizzare l'opzione "Blocca" in Windows che rimanda alla schermata di login senza disconnettere) per proteggere l'accesso alla propria postazione di lavoro nel caso di assenza anche temporanea.

f) Quando possibile, spegnere il PC al termine dell'attività lavorativa giornaliera.

g) Assicurarsi che l'agente di sicurezza endpoint (attualmente BitDefender) sia regolarmente in funzione e non siano presenti allarmi.




h) Prestare attenzione a messaggi di posta elettronica sospetti, di cui non si conosce il mittente e/o che contengono link sospetti o allegati non richiesti, non aprire gli allegati, non seguire i link – in caso di dubbi chiedere supporto ai referenti della UO Tecnologie Informatiche.

i) Disattivare l'esecuzione automatica di contenuti dinamici (es. macro) presenti nei file (in particolare nei documenti Word ed Excel).

j) Disattivare l'anteprima automatica dei contenuti dei file.

k) Segnalare ogni sospetto furto di credenziali, rilevamento virus, tentativo di intrusione o altro abuso ai referenti della UO Tecnologie Informatiche.

l) Fare sempre riferimento ai referenti ai referenti della UO Tecnologie Informatiche per l'installazione e la configurazione di nuovi dispositivi.

m) Leggere gli avvisi e mettere in atto le raccomandazioni di sicurezza diffuse dalla UO Tecnologie Informatiche.

n) In ufficio non lasciare mai il computer portatile incustodito per un periodo di tempo prolungato a meno che non sia riposto al sicuro in un armadio o in un ufficio chiuso a chiave o assicurato alla scrivania tramite un cavo Kensignton. Quando si è viaggio, tenere il computer vicino e non lasciarlo incustodito, non lasciarlo visibile all'interno dell'auto ma eventualmente riporlo nel bagagliaio

Si rimanda altresì alla disposizioni contenute nei seguenti disciplinari:

- "*Disciplinare per l'Utilizzo del Servizio di Posta Elettronica*" approvato con il Decreto nr. 72 del 14/06/2023;
- "*Disciplinare per l'accesso remoto ai sistemi informativi dell'ente*" approvato con il Decreto Decreto n. 135 del 21/12/2022;

## 3) Raccomandazioni di Sicurezza Valide per gli Amministratori di Sistema

Le seguenti raccomandazioni sono rivolte a tutti coloro che hanno accesso con diritti amministrativi e/o di super-utente ad uno o più postazioni di lavoro.

Anche gli amministratori dovranno attenersi a quanto indicato al paragrafo precedente e valide per tutti gli utenti, salvo le seguenti indicazioni specifiche.

Per tutte le operazioni sotto indicate si consiglia di chiedere supporto ai referenti della UO Tecnologie Informatiche.

### a) Uso appropriato dei privilegi di amministratore

- Per le utenze amministrative utilizzare password con lunghezza di almeno 14 caratteri, con combinazioni di lettere numeri e caratteri speciali, e modificarle almeno ogni 3 mesi.
- Impedire che password già utilizzate siano riutilizzate a breve distanza di tempo.
- Se nel dispositivo e negli applicativi sono configurate credenziali di default, provvedere a modificare subito la password.
- Eliminare i profili utente non necessari o dismessi.
- Preferire sempre l'utilizzo di credenziali personali che non abbiano privilegi di amministratore per l'utilizzo ordinario del proprio computer.
- In caso sia necessario utilizzare privilegi di tipo amministrativo, includere il proprio account nel gruppo Windows degli amministratori locali (o nel gruppo dei sudoers per i sistemi Linux/Unix e MacOS).
- Se è necessario autorizzare più profili amministratore, mantenere l'elenco delle utenze amministrative. Ogni credenziale deve essere nominativa e riconducibile ad una sola persona.
- Se la postazione è utilizzata da più utenti, ove possibile, non creare utenti locali ma abilitare l'accesso tramite il servizio Active Directory (o chiederne l'abilitazione ai referenti della UO Tecnologie Informatiche).
- Adottare misure di custodia e protezione adeguate per garantire la disponibilità e la riservatezza della password dell'utenza amministrativa in caso di necessità.
- Non utilizzare la stessa password per utenze o servizi diversi.
- Non comunicare le proprie password ad alcuno.
- Evitare di salvare le password sul sistema operativo, sul browser o su applicativi in uso. accesso (è possibile salvare l'archivio delle password su specifici programmi che fanno uso di tecniche

di cifratura, se interessati chiedere supporto alla UO Tecnologie Informatiche).

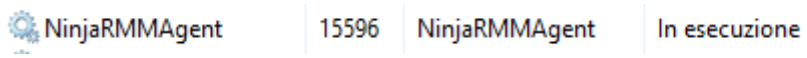
- Disabilitare il boot da rete, USB, dispositivi rimovibili.
- Abilitare solo le condivisioni in rete necessarie all'attività lavorativa e protette mediante l'utilizzo di credenziali di accesso.
- Per l'eventuale amministrazione da remoto attenersi alle disposizioni dello specifico disciplinare.

### b) Inventario dei dispositivi autorizzati

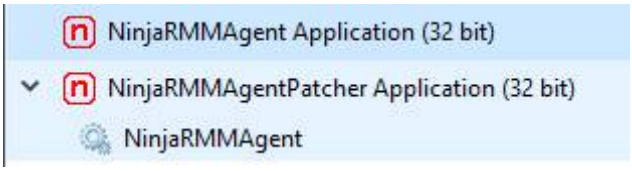
Per fare sì che il dispositivo venga censito nell'inventario generale tenuto dalla UO Tecnologie Informatiche verificare che l'agente di gestione endpoint (attualmente NinjaRMM) sia correttamente installato ed in esecuzione.

In pratica:

- controllare lo stato del servizio NinjaRMMAgent




- controllare che siano in esecuzione i relativi processi




Verificare che l'indirizzo IP della macchina sia fornito dal DHCP. In tutti i casi in cui ciò non sia possibile l'indirizzo IP dovrà essere quello statico richiesto ed assegnato dalla UO Tecnologie Informatiche.

### c) Inventario dei software autorizzati e non autorizzati

Installare solo software autorizzato presente nell'elenco pubblicato sulla Intranet (pagina http://intranet.sede.provincia.pisa.it/software/). Comunicare le eventuali nuove esigenze ai referenti della UO Tecnologie Informatiche che inseriranno il software nella lista degli autorizzati e valuteranno se fossero necessarie particolari misure di sicurezza.

Verificare che l'agente di gestione (NinjaRMM, che mantiene aggiornato l'inventario del software) sia correttamente in esecuzione.

### d) Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

Al fine di utilizzare configurazioni sicure e standard fare sempre riferimento ai referenti della UO Tecnologie Informatiche per l'installazione e la configurazione di nuovi dispositivi e programmi. Segnalare preventivamente ogni esigenza di questo tipo allo scopo di:

- verificare l'esistenza di eventuali requisiti ed ottenere le necessarie indicazioni;
- ottenere le informazioni necessarie per la configurazione;
- ottenere supporto per l'installazione dell'agente di sicurezza e dell'agente di gestione;
- ottenere le licenze del software da installare;

Attenersi puntualmente alla procedura di installazione standard delle PdL pubblicata sulla Intranet che contiene disposizioni per la corretta configurazione di rete, l'integrazione con il dominio, la

rimozione delle utenze locali non necessarie, l'installazione degli agenti di **s**icurezza e gestione e del software di utilità autorizzato.

Collegarsi ai sistemi da amministrare utilizzando protocolli sicuri (HTTPS, SSH, RDP).

### e) Valutazione e correzione continua delle vulnerabilità

Aggiornare costantemente sia il sistema operativo sia le applicazioni installate alle ultime versioni senza vulnerabilità note e alle ultime patch di sicurezza disponibili. Per i sistemi collegati in rete impostare l'aggiornamento automatico. Per i sistemi separati dalla rete effettuare gli aggiornamenti manualmente.

Verificare che l'agente di gestione (NinjaRMM che installa in modo automatico le patch del sistema operativo e dei programmi) sia correttamente in esecuzione.

### f) Difese contro i malware

Fare sempre riferimento ai referenti della UO Tecnologie Informatiche per l'installazione e la configurazione del programma antivirus/antimalware fornito dall'ente (attualmente BitDefender).

Verificare che l'agente di sicurezza (BitDefender) sia correttamente in esecuzione.

Verificare che sia disattivata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.

### g) Copie di sicurezza

Individuare la posizione dei dati e dei documenti da proteggere e fare riferimento ai referenti della UO Tecnologie Informatiche per l'installazione e la configurazione del programma di backup.

Verificare almeno settimanalmente il buon esito dei backup.

Effettuare, con opportuna frequenza (da determinare in base alla frequenza di aggiornamento) una copia dei dati su supporti esterni non siano permanentemente accessibili in rete per evitare che gli attacchi possano coinvolgere anche le copie di sicurezza.

### h) Protezione dei dati

Verificare se la postazione di lavoro contenga dati sensibili o con particolari requisiti di riservatezza, in tal caso impostare la cifratura del disco tramite la funzione di sistema operativo BitLocker e comunicare la chiave di ripristino ai referenti della UO Tecnologie Informatiche.

In caso di dismissione di una postazione di lavoro, disinstallare il software con licenza installato e cancellare in modo sicuro le informazioni contenute nel disco.

## 4) Individuazione degli Amministratori di Sistema

Il Garante della Privacy, con il provvedimento "Misure ed accorgimenti prescritti ai titolari dei trattamenti con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (G.U. n.300 del 24 dicembre 2008) ha prescritto ai titolari dei trattamenti di dati personali effettuati con strumenti elettronici di adottare – fra le altre – le seguenti misure:

- valutare l'esperienza, capacità e affidabilità dei soggetti designati quali amministratori di sistema, nonché la predisposizione al rispetto della normativa;

- indicare, puntualmente, gli ambiti di operatività di ciascun amministratore di sistema;

La Provincia, in applicazione al provvedimento del Garante, con il Decreto Presidenziale n.73 del 15/12/2009:

- ha individuato i funzionari e gli istruttori informatici della UO Tecnologie Informatiche, Fonia e Innovazione quali amministratori di sistema incaricati della gestione delle reti, dei server e dei sistemi di elaborazione dati condivisi dell'ente;
- ha dato facoltà ai Dirigenti ed ai responsabili del trattamento di nominare altri amministratori di sistema, interni o esterni, per i sistemi di elaborazione in dotazione;

Laddove sussistano particolari esigenze organizzative, i dipendenti della Provincia potranno essere designati quali amministratori di sistema delle loro postazioni di lavoro, in tal caso dovranno operare adottando le misure di sicurezza informatica descritte nel presente disciplinare. La richiesta, sottoscritta dall'interessato ed avvallata dal dirigente, dovrà essere indirizzata alla UO Tecnologie Informatiche, Fonia e Innovazione che provvederà alle abilitazioni eventualmente necessarie.

PROVINCIA DI PISA

Settore ……

UO ……

Pisa, data del protocollo

Alla c.a. di
UO Tecnologie Informatiche, Fonia e Innovazione

**Oggetto: DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA INFORMATICA**

Il sottoscritto _____

Dipendente del Settore/Ufficio _____

CHIEDE

Di essere abilitato ad utilizzare con privilegi di amministratore la seguente postazione di lavoro

Nome del PC: _____

Motivo della richiesta: _____

_____

DICHIARA

- di aver ricevuto, letto, compreso e accettato il disciplinare (allegato A) inerente le misure di sicurezza informatica da adottare sulle postazioni di lavoro;
- di assumersi la responsabilità di eventuali incidenti derivanti dalla non applicazione delle disposizioni del suddetto disciplinare.

Il Dipendente

Firma _____

Il DIRIGENTE responsabile

Firma per avallo e conferma _____

PROVINCIA DI PISA

**Istituzione dei Comuni per il governo dell'area vasta**
**Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente**
**Gestione associata di servizi e assistenza ai Comuni**

SETTORE AFFARI E SERVIZI GENERALI. SERVIZI AMBIENTALI E TERRITORIALI.

## PARERE DI REGOLARITA' TECNICA

Sulla proposta di Decreto n. 3753/2024
ad oggetto: DISCIPLINARE INERENTE LE MISURE DI SICUREZZA INFORMATICA DA ADOTTARE SULLE POSTAZIONI DI LAVORO

si esprime ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000, parere FAVOREVOLE in ordine alla regolarita' tecnica.

Pisa li, 13/12/2024

**Sottoscritto dal Dirigente**
(FIORAVANTI PAOLA)
con firma digitale