Linee Guida IT

Titolo:	Linee Guida	**Edizione:**	1
Codice:	P03	**Revisione:**	/
File:	P03 Linee Guida per IT.doc	**Aggiornamento:**	Giugno 2022

Indice

Introduzione

Questo documento intende formalizzare alcune linee guida per il personale dei Sistemi Informativi per garantire il rispetto della vigente normativa in materia di misure minime di sicurezza e per contribuire al raggiungimento degli obiettivi della sicurezza, riassumibili nei tre aspetti distinti:

Disponibilità: ovvero, garantire l'accesso alle informazioni e ai servizi di rete da parte del personale incaricato in relazione alle esigenze lavorative;

Riservatezza: ovvero, garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;

Integrità: ovvero, garantire che le informazioni non siano state alterate da incidenti o abusi.

Il raggiungimento dei suddetti obiettivi richiede un'attenta collaborazione da parte del personale preposto alla gestione e manutenzione dei sistemi informativi con i colleghi delle altre Direzioni.

1. Criteri tecnico – organizzativi e Procedure di Sicurezza

Il Responsabile per i Sistemi Informativi deve attivarsi affinché le misure di sicurezza in seguito descritte siano efficaci. In caso di implementazione di nuovi processi (trattamenti) o di nuovi applicativi, le misure di sicurezza di seguito descritte devono essere efficaci anteriormente all'inizio del trattamento.

In particolare, con riferimento alle attività di individuazione delle esigenze informatiche e sviluppo del piano investimenti e di definizione e gestione dell'architettura dei sistemi informatici si dovrà prestare attenzione agli aspetti attinenti le misure minime di sicurezza; per quanto concerne la realizzazione del piano di sviluppo informatico, allorché quest'ultimo comporti attività di adeguamento ad obblighi normativi in tema di sicurezza informatica, darà – per quanto necessario - precedenza a tali ultimi aspetti al fine di garantire il rispetto dei termini imposti dalle leggi di riferimento.

Per quanto concerne le attività di razionalizzazione delle risorse hardware e software, il Responsabile per i Sistemi Informativi competente si attiva per trovare soluzioni che garantiscano la conformità al dettato legislativo, per quanto possibile, dando preferenza a soluzioni che abbiano un minore impatto in termini di costi, di modifica dei processi aziendali o delle prassi seguite dagli incaricati del trattamento.

In caso di accordi di service con società esterne, nell'ambito delle attività di gestione di tali contratti, il Responsabile per i Sistemi Informativi vigilerà sulla conformità dei servizi resi rispetto alle misure minime di sicurezza di natura organizzativa, fisica e tecnologica.

Per lo svolgimento di tali attività il Responsabile per i Sistemi Informativi si avvale della collaborazione degli Amministratori di Sistema, dei Custodi delle chiavi logiche e si coordina con gli altri Responsabili del trattamento.

2. Trattamento dei Dati Personali Effettuato con Strumenti Elettronici o Comunque Automatizzati

2.1. Nomina degli Amministratori di sistema

Il Titolare del trattamento provvede ad individuare per iscritto tutti gli incaricati che svolgano funzioni di Amministratori di Sistema, nonché coloro i quali siano preposti agli accessi alle informazioni concernenti le password degli utenti/incaricati.

Gli accessi alle password o ai documenti che contengono le password degli utenti/incaricati devono essere limitati a quanto strettamente necessario per garantire la disponibilità di risorse o servizi. In particolare, tali accessi potranno avvenire solo nei seguenti casi:

- specifica richiesta dell'utente/incaricato (per esempio: per casi di dimenticanza, malfunzionamenti o, più in generale per scopi di manutenzione richiesta dall'incaricato/utente);
- specifica richiesta del responsabile del Trattamento d'Ufficio cui fa parte l'incaricato titolare della password (per esempio: per casi eccezionali nei quali si rende necessario provvedere al recupero di informazioni, documenti o risorse, quali morte, infermità o assenza prolungata, richieste dell'Autorità Giudiziaria o di Pubblica Sicurezza, ecc.);
- specifica richiesta del responsabile del Trattamento per la Direzione/Divisione cui fa parte l'incaricato titolare della password.

In tali casi, prima dell'accesso, l'Amministratore di sistema provvederà ad avvertire l'utente titolare del documento o delle informazioni oggetto dell'intervento. Laddove ciò non sia possibile, provvederà ad inviargli una comunicazione circa l'intervento effettuato tramite posta elettronica.

Le password inerenti la funzione "administrator" dei sistemi operativi non devono essere condivise con gli incaricati non previamente individuati per iscritto come amministratori di sistema. In caso di perdita di riservatezza di tale password, gli Amministratori di Sistema – per quanto di sua competenza – provvederà immediatamente a modificarle.

Nello svolgimento delle proprie funzioni e, in particolare, nello svolgere le attività di manutenzione di sistemi hardware o software, gli Amministratori di sistema e gli incaricati della manutenzione sono tenuto al massimo riserbo in merito alle informazioni di cui possono venire a conoscenza.

Qualora l'attività di manutenzione sia svolta da personale esterno all'organizzazione, il Responsabile del trattamento competente provvederà – direttamente o indirettamente – a controllare l'operato degli addetti alla manutenzione.

3. Credenziali di Autenticazione

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché il trattamento di dati personali con strumenti elettronici sia consentito ai soli Incaricati dotati di credenziali di autenticazione, che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché per l'accesso alle risorse di rete e agli applicativi preposti al trattamento di dati personali esistano procedure di autenticazione relative a specifici trattamenti o a più trattamenti.

Le credenziali di autenticazione devono consistere in un codice per l'identificazione di un incaricato associato a una parola chiave riservata conosciuta esclusivamente dal medesimo, ovvero in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (es. smart card, token), eventualmente associato a un codice identificativo o a una parola chiave, ovvero in un sistema biometrico dell'incaricato (es. impronta digitale, retina), eventualmente associata a un codice identificativo o a una parola chiave.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché ad ogni incaricato siano assegnate o associate individualmente una o più credenziali per l'autenticazione.

Si ricorda che l'accesso ai dati personali registrati in elaboratori (PC, server, ecc.) deve essere riservato al personale che sia stato individuato come Incaricato al trattamento di dati personali dal Responsabile del trattamento per i dati del personale.

Parole Chiave (password)

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché la parola chiave, quando è prevista dal sistema di autenticazione, sia composta da almeno 8 caratteri. La parola chiave, nel caso in cui lo strumento elettronico non permetta otto caratteri, dovrà essere composta da un numero di caratteri pari al massimo consentito.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché sia rispettata di fatto la regola, che la Società ha provveduto a formalizzare, inerente il divieto di comporre la parola chiave con riferimenti agevolmente riconducibili all'incaricato (es. nome, data di nascita, nomi di familiari).

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché la parola chiave sia modificata dagli Incaricati al primo utilizzo e, successivamente, almeno ogni 6 mesi. La parola chiave, nel caso di trattamento di dati sensibili e di dati giudiziari, dovrà essere modificata almeno ogni 3 mesi.

Laddove possibile, in base alle tecnologie utilizzate, gli Amministratori di Sistema provvedono affinché ogni incaricato possa modificare la propria password autonomamente. Nel caso di password di BIOS, all'atto della modifica della propria password, gli incaricati dovranno comunicare in busta chiusa ai custodi delle chiavi logiche la password modificata e questi ultimi dovranno custodirla in modo riservato per renderle accessibili in caso d'uso.

Codici Identificativi

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, provvede affinché il codice per l'identificazione degli incaricati o utenti di rete, laddove utilizzato, non sia assegnato ad altri incaricati, neanche in tempi diversi.

Disattivazione delle credenziali

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché le credenziali di autenticazione non utilizzate da almeno 6 mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (password di "*administrator*"). Le credenziali dovranno essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Sistema e profili di autorizzazione

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso deve essere utilizzato un sistema di autorizzazione. I profili di autorizzazione possono essere impostati per singolo incaricato o per classi omogenee di incaricati e devono essere individuati e configurati anteriormente all'inizio del trattamento in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

La sussistenza delle condizioni per la conservazione dei profili di autorizzazione sarà verificata periodicamente e comunque almeno annualmente.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché la lista degli incaricati e degli addetti alla gestione o alla manutenzione degli strumenti elettronici, nonché i relativi profili di accesso siano aggiornati periodicamente e almeno annualmente (anche per classi omogenee di incarico e relativi profili di accesso).

Sistemi di sicurezza e antivirus

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché siano implementati strumenti elettronici per garantire la protezione dei dati personali contro il rischio di intrusione (firewalling) e dell'azione di virus o software dannosi.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché tali strumenti siano aggiornati con cadenza almeno semestrale (patches di sicurezza, service pack), previa installazione di verifica in ambiente di test.

I sistemi antivirus siano installati e attivi su tutti gli elaboratori e devono essere strutturati affinché sia attivo e garantito il processo di aggiornamento automatico. Devono essere adottate soluzioni tecniche affinché gli incaricati non possano disattivare tali sistemi.

Semestralmente, gli Amministratori di Sistema verificano l'efficacia e l'aggiornamento di detti strumenti, redigendo, al termine della verifica, un verbale che dovrà essere trasmesso al Responsabile dei Sistemi Informativi.

Il verbale di verifica dovrà attestare che tutti gli elaboratori sia installato ed attivo un software antivirus, nonché il buon funzionamento delle procedure di aggiornamento del software stesso, ovvero segnalare eventuali difformità riscontrate. In caso di difformità o malfunzionamenti delle procedure software di aggiornamento, gli Amministratori di Sistema provvederanno a porre rimedio a tali disfunzioni o difformità.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché le categorie particolari di dati personali o i dati giudiziari siano protetti contro l'accesso abusivo, di cui all' articolo 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici (firewall e sistemi di identificazione e profilazione accessi).

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, predispone i sistemi informatici e telematici affinché gli strumenti utilizzati per l'interconnessione e scambio di dati sensibili in via telematica siano solamente quelli prefigurati ed autorizzati.

Aggiornamenti periodici programmi per elaboratore

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (es. service pack e patches) siano aggiornati almeno semestralmente. Quanto sopra sarà oggetto di verifica ispettiva periodica.

Back-up e ripristino dei dati

I dati contenuti nei dischi fissi dei sistemi centrali server sono sottoposti a salvataggio con frequenza giornaliera; le copie sono catalogate, datate e conservate in armadi chiusi a chiave in locali diversi da quelli in cui sono istallati i server.

Qualora gli incaricati abbiano documenti salvati sui dischi fissi è necessario che gli stessi almeno settimanalmente effettuino un salvataggio in rete dei medesimi documenti.

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché siano impartite istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale. Inoltre, gli Amministratori di Sistema provvedono a gestire i sistemi e le procedure di back-up in modo che sia garantito il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

I supporti di backup e le riproduzioni digitali contenenti dati personali o sensibili devono essere conservati e custoditi con le medesime modalità previste per i documenti originali e/o per i sistemi di provenienza.

Supporti rimuovibili e dismissione elaboratori

Il Responsabile per i Sistemi Informativi, tramite gli Amministratori di Sistema, dispone affinché siano impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

Gli Amministratori di Sistema sono tenuti a distruggere o rendere inutilizzabili i supporti rimovibili e/o le memorie degli elaboratori contenenti dati sensibili o giudiziari non più utilizzati. I supporti rimovibili contenenti dati sensibili o giudiziari potranno essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, esclusivamente nell'ipotesi in cui le informazioni non siano intelligibili e tecnicamente in alcun modo ricostruibili (formattazione a basso livello).

I supporti dismessi o consegnati a terzi per scopi di manutenzione devono essere controllati per verificare l'eliminazione di eventuali dati personali o sensibili, salvo che l'intervento di manutenzione presso terzi sia finalizzato proprio al recupero di tali informazioni.

Affidamento a terzi per implementazione di misure minime di sicurezza

Qualora ci si avvalga di soggetti esterni alla struttura aziendale per adottare adeguate misure di sicurezza, il Responsabile dei Sistemi Informativi provvede, qualora il titolare del trattamento lo abbia ritenuto opportuno, a farsi rilasciare dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità rispetto alle misure che il Titolare del trattamento abbia ritenuto adeguate sulla base delle risultanze dell'analisi dei rischi.

Controlli periodici, analisi dei rischi e Registro dei trattamenti

Il Responsabile dei Sistemi Informativi collabora con le altre funzioni aziendali per effettuare e verbalizzare i controlli periodici previsti dall'organizzazione e per la miglior riuscita delle attività inerenti l'analisi dei sistemi informativi aziendali, l'analisi dei rischi e la stesura del Registro dei trattamenti.

Elaboratori destinati ad accessi da parte di più soggetti autorizzati

Eventuali elaboratori di utilizzo comune da parte di diversi incaricati (per esempio in quanto eroganti servizi informativi, come gli accessi a basi dati pubbliche), devono essere configurati con sistemi operativi che gestiscano le diverse profilazioni di accesso. In alternativa, tali elaboratori non devono contenere dati personali, né poter accedere a risorse o applicativi contenenti dati personali, salvo che i medesimi dati siano pubblici o conoscibili da chiunque.