# STRATESIS

# Security Company

Sistema di gestione per la sicurezza delle informazioni

Norma di riferimento: UNI ISO/IEC 27001:2017

## Politica di sicurezza delle Informazioni

[ **X** ] **Copia Controllata n° __ Rev. 0** [ ] Copia Non Controllata n°(*facoltativo*)

Destinatari

Data distribuzione 07.09.2022



## REGISTRO DELLE REVISIONI

| DATA | REV. | OGGETTO DELLA MODIFICA |
|---|---|---|
| | | |
| | | |
| 07.09.2023 | 0 | PRIMA EMISSIONE |

## ITER DI EMISSIONE

| | NOME | FUNZIONE | FIRMA |
|---|---|---|---|
| REDATTA DA | MEMOLE INGEGNERIA S.R.L. | SOCIETÀ CONSULENZA | |
| APPROVATA DA | GIANFRANCO ROATI | DIREZIONE | |

# Sommario

## 1. Dichiarazione sulla politica di sicurezza delle informazioni (A.7.2.1)

La direzione STRATESIS si impegna a trasmettere e a fare applicare ai propri dipendenti la seguente politica sulla sicurezza delle informazioni.
Lo scopo della politica è quello di proteggere le risorse informatiche di STRATESIS e i suoi clienti da tutte le minacce, interne o esterne, intenzionali o accidentali.

La gestione di STRATESIS ha approvato questa politica.
Con questa politica, l'intento di STRATESIS è garantire che:

- Le informazioni siano protette contro l'accesso non autorizzato
- Sia garantita la riservatezza delle informazioni
- Sia mantenuta l'integrità delle informazioni
- Sia garantita la disponibilità delle informazioni
- Siano rispettati i requisiti normativi e legislativi
- Tutte le violazioni della sicurezza delle informazioni, reali o sospette, siano segnalate e analizzate
- Siano definiti standard per sostenere la politica. Questi standard includono controlli di virus e password
- Siano rispettati i requisiti aziendali per la disponibilità di informazioni e sistemi informatici

È compito diretto del responsabile del reparto Infrastruttura Tecnologica mantenere la politica e fornire consigli e indicazioni sulla sua attuazione.

Tutti i Referenti sono direttamente responsabili dell'attuazione della politica all'interno delle proprie aree di business e dell'osservanza da parte del rispettivo personale.
Questa politica è applicabile anche ai sistemi esterni (cliente) ai quali i dipendenti STRATESIS hanno accesso, a meno che non sia in contraddizione con la politica di sicurezza delle informazioni del cliente.

STRATESIS garantisce che siano mantenute la riservatezza, l'integrità e la disponibilità delle informazioni, mediante l'attuazione delle migliori prassi per ridurre al minimo il rischio.
È responsabilità di ciascun dipendente STRATESIS aderire alla politica della sicurezza.

## 2. Introduzione

Questa politica è stata sviluppata per proteggere tutti i sistemi all'interno di STRATESIS da eventi che possono mettere a rischio l'attività aziendale. Questi eventi includono gli incidenti così come un comportamento deliberatamente progettato per causare difficoltà.

### *2.1. Sicurezza delle Informazioni*

Sicurezza delle informazioni significa proteggere informazioni e sistemi informatici da accesso, utilizzo, divulgazione, interruzione, modifica o distruzione non autorizzati. L'obiettivo della sicurezza delle informazioni è quello di garantire la continuità del business e ridurre al minimo i danni prevenendo e minimizzando l'impatto degli incidenti relativi alla sicurezza.
Le informazioni assumono molte forme e includono i dati memorizzati sui computer, trasmessi attraverso le reti, stampati o scritti su carta, inviati via fax, memorizzati su qualsiasi supporto o comunicati in una conversazione o per telefono.
Tre concetti chiave costituiscono i principi fondamentali della sicurezza delle informazioni: riservatezza, integrità e disponibilità. Questi concetti sono conosciuti come triade CIA.

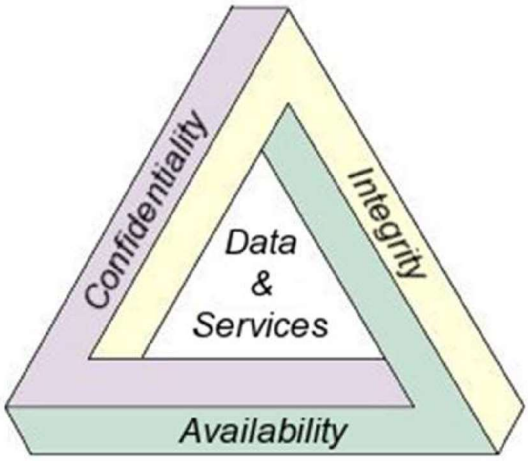


**Figura 1 – Triade CIA**

### 2.1.1. Riservatezza

Alle informazioni considerate riservate in natura sono consentiti l'accesso, l'utilizzo, la copia o la divulgazione solo da parte di persone che sono state autorizzate ad accedere, utilizzare, copiare o divulgare le informazioni, e solo quando vi è una reale necessità di accedere, utilizzare, copiare o divulgare tali informazioni. Una violazione della riservatezza si verifica quando alle informazioni considerate riservate in natura è stato o potrebbe essere stato eseguito l'accesso, l'utilizzo, la copia o la divulgazione da parte di qualcuno che non era autorizzato ad avere accesso a tali informazioni.
La riservatezza è garantita proteggendo informazioni preziose o sensibili da divulgazione non autorizzata o interruzione intelligibile.

### 2.1.2. Integrità

In ambito della sicurezza delle informazioni, integrità significa che i dati non possono essere creati, modificati o eliminati senza autorizzazione.
L'integrità è garantita salvaguardando l'accuratezza e la completezza delle informazioni, proteggendo tali informazioni da modifiche non autorizzate.

### 2.1.3. Disponibilità

Il concetto di disponibilità indica che le informazioni, i sistemi informatici utilizzati per elaborare le informazioni ed i controlli di sicurezza utilizzati per proteggere le informazioni sono tutti disponibili e funzionano correttamente quando le informazioni sono necessarie.

## *2.2. Prescrizioni di legge*

Gli utenti devono essere a conoscenza della normativa riportata qui di seguito e delle loro responsabilità sia personali che per conto dell'Autorità nel trattamento di dati, hardware e software.

### 2.2.1. Tutela dei dati personali sensibili

Chiunque elabori o utilizzi le informazioni personali deve rispettare i seguenti principi come definiti nella legge (per l'Italia, questo principio è disciplinato dalla legge sulla privacy n.
196/2003 E SMI e dal Regolamento generale sulla protezione dei dati - GDPR, Regolamento UE 2016/679).
I dati personali devono essere:

- Trattati in modo corretto e lecito
- Ottenuti per finalità determinate e legittime e trattati solo in conformità con la notifica al Garante
- Adeguati, pertinenti e non eccessivi
- Accurati e, se necessario, aggiornati
- Conservati per il tempo strettamente necessario

- Trattati in conformità con i diritti dei singoli
- Mantenuti al sicuro con le misure adottate per evitare il trattamento non autorizzato

I dati sensibili devono essere trattati solo se i singoli hanno dato il loro consenso esplicito. I singoli hanno in conformità con le disposizioni della legge, il diritto di accedere ai propri dati personali.

#### 2.2.2. Uso improprio del computer

Questa legge definisce reati specifici relativi all' "hacking" (Direttiva UE 98/84/CE, D.Lgs 15 novembre 2000, n. 373). Pertanto, anche l'intento di eseguire l'accesso non autorizzato a programmi o dati in un computer è reato se il trasgressore è consapevole che l'accesso non è autorizzato e il computer ha la funzione di eseguire determinate azioni (anche semplici come lo scorrimento dello schermo). I dipendenti che hanno accesso autorizzato non hanno l'autorità di conferire o autorizzare l'accesso ad altri. È reato anche incitare qualcuno a conferire accesso non autorizzato. Allo stesso modo, è reato causare modifiche non autorizzate a programmi e dati, che comportano l'introduzione deliberata di un virus.

#### 2.2.3. Diritto d'autore, disegni e brevetti

Questo concetto è collegato alla Direttiva UE 2004/48/CE, legge n. 633 del 22 aprile 1941 (insieme a vari emendamenti) e al codice civile italiano, che specificano i reati relativi alla copia illegale di software. Tutte le organizzazioni hanno la responsabilità legale di garantire che tutto il software sia concesso in licenza da parte del fornitore che detiene i diritti d'autore per il prodotto. Le organizzazioni hanno la responsabilità di tenere registri adeguati che dimostrino la conformità. La politica dell'organizzazione deve garantire che nessun materiale protetto da copyright venga copiato senza il consenso del proprietario.
Questa legge viene applicata da organizzazioni come FAST (Federation against Software Theft) e BSA (Business Software Alliance) che hanno ampi poteri per garantire la conformità.

#### 2.2.4. ISO27001 - Tecniche per la sicurezza-sistemi di gestione per la sicurezza delle informazioni

Questa normativa, sviluppata nel 2005, specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di una organizzazione, indipendentemente dalla tipologia, dimensione e natura.
STRATESIS ha implementato un sistema di gestione per la sicurezza delle informazioni conforme a tale schema.

### *2.3. Necessità di una politica di sicurezza delle informazioni*

I dati memorizzati nei sistemi utilizzati da STRATESIS rappresentano una risorsa estremamente preziosa. A causa della crescente dipendenza dalla tecnologia informatica, è necessario garantire che questi sistemi siano sviluppati, operati, utilizzati e mantenuti in modo sicuro e protetto. La necessità sempre più frequente di trasmettere informazioni attraverso la rete rende i dati più vulnerabili a modifiche o divulgazioni, accidentali o intenzionali, non autorizzate.
Questa politica di sicurezza delle informazioni ha lo scopo di informare i dipendenti STRATESIS delle azioni consentite e vietate per evitare eventuali incomprensioni e controversie future, correlate in particolare a richieste da parti esterne.
***La sicurezza delle informazioni in STRATESIS è basata sul fatto che tutte le azioni correlate alla sicurezza che non sono esplicitamente consentite devono essere considerate vietate.***
Il livello di sicurezza richiesto in un particolare sistema dipende dai rischi associati al sistema, dai dati presenti nel sistema e dall'ambiente di lavoro del sistema.
Questa politica si applica a tutte le informazioni in formato fisico ed elettronico.

### *2.4. Obiettivi della politica di sicurezza (A.5.1.1-A.5.1.2)*

Gli obiettivi della politica di sicurezza delle informazioni STRATESIS sono:

- Garantire che tutti i dipendenti abbiano una giusta consapevolezza e preoccupazione per la sicurezza dei sistemi informatici e un'adeguata percezione delle proprie responsabilità per la sicurezza informatica
- Garantire che tutti gli appaltatori e i loro dipendenti abbiano una giusta consapevolezza e preoccupazione per la sicurezza delle informazioni STRATESIS
- Fornire un quadro contenente i concetti per stabilire standard, procedure e strutture informatiche per l'implementazione della sicurezza dei sistemi informatici
- Soddisfare gli obiettivi generali per la sicurezza dei sistemi informatici contenuti nella norma ISO 27001
- Specificare le responsabilità di STRATESIS
- Garantire che tutto il personale abbia consapevolezza della legge sulla protezione dei dati e delle sue implicazioni
- Garantire che tutto il personale abbia consapevolezza della legge sull'uso improprio del computer
- Garantire che tutto il personale sia consapevole delle proprie responsabilità e che il mancato rispetto della politica di sicurezza delle informazioni sia un illecito disciplinare che può comportare azioni fino al licenziamento.

### *2.5. Quali sono i soggetti interessati dalla politica (A.7.1.2)*

La politica si applica a tutti i dipendenti di STRATESIS. Si applica anche agli appaltatori e ai visitatori, non dipendenti di STRATESIS, ma che sono impegnati a lavorare con STRATESIS o che hanno accesso a informazioni di STRATESIS o presenti sui suoi sistemi o sui sistemi a cui STRATESIS è autorizzata ad accedere.
La politica si applica a tutti i luoghi da cui si accede ai sistemi STRATESIS (compreso l'uso domestico o altri usi remoti). Laddove sono presenti collegamenti che consentono alle organizzazioni non STRATESIS di avere accesso alle informazioni STRATESIS, STRATESIS deve confermare che le politiche di sicurezza in cui si opera soddisfino i requisiti di sicurezza o che il rischio sia conosciuto e mitigato.
Se la politica di sicurezza del cliente STRATESIS è più severa, i dipendenti STRATESIS che lavorano per quel cliente si atterranno a tali regole più severe.
La politica si applica a tutti i sistemi e tutte le informazioni.

### *2.6. Uso accettabile*

L'uso di tutti i sistemi informatici sarà conforme alla politica sull'uso accettabile. L'uso accettabile è definito come l'uso a fini di:

- Lavoro di sviluppo e comunicazione ad esso associata
- Ricerca
- Sviluppo educativo personale
- Amministrazione e gestione
- Attività di consulenza contratta per STRATESIS

L'uso ragionevole delle strutture informatiche per la corrispondenza personale, laddove non connesso ad alcuna attività commerciale, è attualmente considerato accettabile.
La politica STRATESIS prevede che tutto l'uso delle strutture debba essere lecito, onesto e decoroso e tenere conto dei diritti e della sensibilità di altre persone.

### *2.7. Riesame e controllo*

È compito del responsabile del reparto Infrastruttura Tecnologica eseguire il riesame periodico della politica alla luce delle circostanze mutevoli. Il riesame viene effettuato ogni anno o quando si verificano modifiche significative.
La gestione STRATESIS ha il compito di garantire che la politica sia appropriata per la tutela degli interessi STRATESIS. Esistenza e modifiche della politica STRATESIS saranno comunicati a tutti i dipendenti attraverso i canali regolari, mentre la sensibilizzazione viene aumentata mediante l'approvazione obbligatoria da parte di ciascun dipendente.

## 3. Accesso alla rete (A.9.1.1)

### *3.1. Accesso ai sistemi (A.9.4.1)*

Il personale STRATESIS e i dipendenti esterni devono accedere solo ai sistemi per cui sono autorizzati.
Secondo l'uso improprio del computer, è reato penale tentare di ottenere l'accesso a informazioni e sistemi informatici per cui non si dispone dell'autorizzazione. Tutti i contratti di lavoro e le condizioni di contratto per parti esterne devono avere una clausola di non divulgazione, che implica che, in caso di accesso non autorizzato accidentale alle informazioni, il membro del personale o dipendente esterno non possa divulgare le informazioni che non aveva diritto di ottenere.
Ad eccezione dell'accesso al materiale destinato al grande pubblico, l'uso di sistemi informatici e reti deve essere limitato solo agli utenti registrati.

### *3.2. Registrazione di utenti*

Procedure formali vengono utilizzate per controllare l'accesso ai sistemi. Un gestore autorizzato deve approvare ogni richiesta di accesso. Il reparto di Infrastruttura Tecnologica è responsabile dell'apertura di nuovi account utente su richiesta del gestore autorizzato. Il livello di accesso è determinato dal reparto di Infrastruttura Tecnologica in base alle competenze di ciascun dipendente, definite dalla direzione I privilegi di accesso saranno modificati o rimossi, a seconda dei casi, quando un singolo cambia mansione o lascia l'impiego, solo su richiesta del dirigente autorizzato.
Gli ospiti non possono accedere alla rete interna dell'azienda.
I dipendenti invece possono accedere alla rete Dati, che consente l'accesso al repository aziendale e ai dati dopo aver richiesto la registrazione al reparto IT.

#### 3.2.1. Procedura di registrazione alla rete Dati

Dopo aver fatto la richiesta di creazione di un nuovo utente al reparto IT, quest'ultimo procede alla configurazione dell'account sui sistemi di autenticazione e al controllo delle autorizzazioni necessarie in base al ruolo che deve avere l'utente stesso.

### *3.3. Gestione utente/password (A.9.3.1 - A.9.4.3)*

Una password è un'informazione di autenticazione riservata costituita da una stringa di caratteri" utilizzata per accedere ai sistemi informatici.

Le password devono essere mantenute riservate. Le password sono di responsabilità dei singoli utenti; non devono essere utilizzate da nessun altro nemmeno per un breve periodo di tempo.
L'utente deve garantire che la password non sia facilmente "individuabile", che non sia scritta su nessun documento accessibile e che segua le indicazioni qui sotto riportate. Fornire una password autorizzata a una persona non autorizzata al fine di ottenere l'accesso a un sistema informatico è un illecito disciplinare.
In merito alle password, il sistema in uso è impostato per fare in modo che gli utenti possano gestire la propria password secondo i seguenti criteri di efficacia:

- La password deve contenere almeno 7 caratteri;
- deve essere una combinazione di caratteri alfanumerici (lettere e numeri) e simboli:
  - Lettere maiuscole (maiuscole). Esempi: A, E, R
  - Lettere minuscole (piccole). Esempi: a, e, r
  - Numeri. Esempi: 2, 6, 7
  - Simboli e caratteri speciali. Esempi:! @ & *
- Non devono contenere il nome account dell'utente o parti del nome completo dell'utente;

Inoltre il sistema di default prevede che l'utente non possa impostare una delle password usate in precedenza e che sia obbligato al cambio password ogni 90gg.

***È buona norma utilizzare password per gli 'screensaver' in uffici con più occupanti ed essenziale nelle aree comuni.***
Nessun membro del personale deve avere accesso a un sistema di produzione a meno che non sia adeguatamente formato e reso consapevole delle proprie responsabilità relative alla sicurezza.
Il personale IT non può mai chiedere agli utenti le loro password.
Il controllo degli account STRATESIS, dei diritti di accesso e delle autorizzazioni viene effettuato almeno due volte l'anno o a richiesta.

### *3.4. Lavoro a domicilio o telelavoro (A.6.2.2)*

L'accesso a Internet comporta un rischio per la sicurezza, in quanto è possibile scaricare virus o programmi in grado di effettuare ricerche sul pc ed intercettare password o altre informazioni.

*L'accesso VPN è concesso dal responsabile del reparto di Infrastruttura Tecnologica su previa approvazione del dirigente responsabile. Quando a un dipendente viene concesso l'accesso, gli viene rilasciato un certificato, che deve essere utilizzato per stabilire la comunicazione VPN. Il certificato può essere revocato senza preavviso se l'accesso viene utilizzato in modo non corretto, se si mette in pericolo la sicurezza della rete Stratesis o se non è più necessario.*
*L'accesso dall'esterno avviene tramite autenticazione VPN.*

#### 3.4.1. Trasporto di hardware, dati e documenti riservati (A.8.3.3, A.11.2.5)

I dipendenti devono, con ragionevole cura, ridurre al minimo il rischio di furto o danneggiamento di hardware, dati e documenti riservati durante il trasporto. L'apparecchiatura IT deve essere trasportata in un ambiente pulito, sicuro. Durante il trasferimento dell'apparecchiatura tra casa e luogo di lavoro, i dipendenti devono tenere l'apparecchiatura fuori dalla vista e non lasciarla mai incustodita. Nessun dispositivo HW aziendale deve essere lasciato in auto durante la notte.

#### 3.4.2. Conservazione (A.11.2.6)

I dipendenti devono adottare tutte le misure ragionevoli per ridurre al minimo la visibilità dei computer da fuori casa e chiudere perfettamente porte e finestre quando la casa non è occupata.
Sarebbe opportuno mettere al sicuro dati confidenziali o relazioni che non vengono utilizzati frequentemente nella zona più protetta della casa.

### *3.5. Personale che lascia l'impiego in STRATESIS (A.7.3.1 e A.8.1.4)*

Prima che un dipendente lasci l'impiego o cambi mansioni, il dirigente responsabile deve assicurarsi che:

- Il dipendente venga informato che continua ad essere vincolato dall'accordo di riservatezza firmato;
- Tutti gli account e le password vengano rimossi o modificati per negare l'accesso;

- I reparti competenti siano informati della cessazione del rapporto di lavoro o del cambiamento delle mansioni e, se necessario, il nome venga rimosso dagli elenchi di autorizzazioni e accessi;
- Le password dei supervisori assegnate al singolo dipendente siano rimosse e venga considerata la possibilità di modificare le password di livello più elevato a cui il dipendente ha accesso;
- Il personale della reception e altri responsabili del controllo dell'accesso ai locali interessati vengano informati della cessazione del rapporto di lavoro e istruiti a non ammettere in futuro il dipendente senza un pass visitatori;
- Le proprietà aziendali vengano restituite;
- Ove necessario i clienti vengano informati, in modo che vengano eliminati o disabilitati anche i loro account e restituiti i token di accesso dei clienti.

Particolare attenzione deve essere posta al momento della restituzione o della disabilitazione di oggetti che potrebbero consentire l'accesso futuro. Questi oggetti includono dispositivi di identificazione personale, schede di accesso, chiavi, Badge, manuali e documenti, HW di proprietà aziendale.
Il reparto di Infrastruttura Tecnologica eliminerà o disabiliterà, nel loro ultimo giorno di lavoro, tutti i codici identificativi e le password dei membri del personale che lasciano l'impiego in STRATESIS. Prima che il membro del personale lasci l'impiego, il responsabile deve garantire che tutti i file di continuo interesse per l'attività di STRATESIS vengano trasferiti ad un altro utente.
Il reparto di Infrastruttura Tecnologica tiene traccia di tutti gli accessi e della modifica degli stessi.

In alcuni casi in cui il dipendente che lascia l'impiego conserva un rapporto formale con STRATESIS, a tale dipendente può essere consentito l'accesso agli account STRATESIS dopo che ha lasciato l'impiego, per un periodo limitato di tempo.

### *3.6. Sicurezza di accesso di terzi (A.11.1)*

Presso le sedi operative, si possono ricevere clienti solo ed esclusivamente su appuntamento e devono essere accolti esclusivamente nella sala riunioni all'entrata. Pertanto il personale è edotto che l'accesso è consentito solo in questi termini.
I visitatori non devono mai essere in grado di visualizzare casualmente schermi di computer o documenti stampati prodotti da un sistema informatico senza autorizzazione. I dirigenti hanno la responsabilità di informare il reparto di Infrastruttura Tecnologica quando il personale temporaneo lascia l'impiego.
Il reparto di Infrastruttura Tecnologica si occupa della manutenzione delle apparecchiature informatiche e software dei dipendenti.
A nessuna parte esterna è consentito l'accesso alle reti STRATESIS, a meno che l'ente non sia autorizzato formalmente. Tutte le parti esterne saranno tenute a firmare accordi di sicurezza e di riservatezza con STRATESIS.
STRATESIS controlla tutto l'accesso esterno ai propri sistemi attivando o disattivando le connessioni per ogni prescrizione di accesso autorizzato.
STRATESIS ha in atto procedure adeguate per assicurare la protezione di tutte le informazioni da inviare ai sistemi esterni. In tal modo, non verrà fatta alcuna ipotesi sulla qualità della sicurezza utilizzata da terzi, ma verrà richiesta conferma dei livelli di sicurezza mantenuti da tali terzi.
Laddove i livelli di sicurezza sono ritenuti inadeguati, saranno utilizzati metodi alternativi per l'invio dei dati.
Tutti i terzi ed eventuali attività in outsourcing sono ritenuti responsabili allo stesso livello di riservatezza del personale STRATESIS.

### *3.7. Sicurezza della rete (A.13.1)*

È compito del responsabile del reparto di Infrastruttura Tecnologica garantire che i diritti di accesso e il controllo del traffico su tutte le reti STRATESIS siano mantenuti correttamente. L'accesso ai sistemi è controllato a più livelli:

- Accesso solo tramite autenticazione utente
- Accesso consentito solo ad informazioni prestabilite per ogni utente
- Sistemi di alert e Log di controllo

Controllo degli accessi Attraverso le regole di firewall;

Rientra nella politica e nella pratica di STRATESIS consentire l'accesso a tutte le informazioni sensibili solo attraverso protocolli di rete sicuri (ad esempio SSL, HTTPS, FTPS, IPsec). Non è possibile l'accesso esterno mediante protocolli non sicuri alla rete STRATESIS (ad esempio, RDC, FTP).
Per l'accesso alla rete internet in azienda, i dipendenti non devono impostare manualmente gli indirizzi IP sulle proprie interfacce di rete. Tali indirizzi devono essere assegnati automaticamente dal server DHCP.

I gestori di progetti e servizi hanno il compito di mantenere il responsabile del reparto di Infrastruttura Tecnologica informato sulle loro esigenze. Ciò comprende numero e nomi degli utenti, i loro requisiti di accesso in termini di tempi e luoghi, le attività che richiedono il supporto di rete e le esigenze degli appaltatori di supporto.
I gestori di progetti e servizi devono mantenere il responsabile del reparto di Infrastruttura Tecnologica informato di nuovi utenti che richiedono l'accesso e di utenti che non hanno più necessità di accesso perché cambiano lavoro o lasciano l'impiego in STRATESIS.
È compito del responsabile del reparto di Infrastruttura Tecnologica garantire che le comunicazioni di dati su reti remote e strutture informatiche non compromettano la sicurezza dei sistemi STRATESIS.

## 4. Sicurezza hardware (A.11.2)

L'accesso alla suite di computer principale, al locale server secondario e ai locali contenenti comunicazioni di dati di apparecchi telefonici deve essere controllato e limitato. L'autorizzazione per accedere a queste aree è controllata dal responsabile del reparto di Infrastruttura Tecnologica. Il controllo degli accessi è effettuato mediante serratura con chiave. Le apparecchiature di comunicazione sono posizionate in ambienti dedicati.
L'hardware fornito a Stratesis dai clienti viene trattato con maggiore cura dell'hardware di proprietà di Stratesis. L'hardware riservato è conservato in locali chiusi a chiave e è accessibile solo ai dipendenti autorizzati.

### *4.1. Sicurezza delle apparecchiature*

I server contenenti informazioni aziendali sono tenuti in un ambiente sicuro, protetto da:
- Sicurezza fisica e controllo degli accessi;
- Dispositivi di spegnimento di incendi;
- Alimentazione elettrica condizionata stabile protetta da gruppo di continuità;

Le apparecchiature di comunicazione chiave saranno anche protette da gruppo di continuità.
Le informazioni elettroniche sono mantenute sui server approvati dal reparto di Infrastruttura Tecnologica.
In ufficio non sono presenti workstation fisse in quanto tutto il personale è dotato di computer portatili di cui è ritenuto diretto responsabile al presidio.

Nessun hosting esterno può avvenire senza approvazione preventiva.
L'apparecchiatura IT deve essere sempre installata e posizionata in accordo alle specifiche del produttore. L'apparecchiatura deve essere sempre installata dal servizio di Infrastruttura Tecnologica o con il permesso del servizio di Infrastruttura Tecnologica.
Fumare, bere e mangiare non è permesso nelle aree che ospitano apparecchiature informatiche.

### *4.2. Apparecchiature informatiche portatili e palmari (A.6.2.1)*

Apparecchiature, dati o software non devono essere portati fuori sede dal personale senza l'autorizzazione di gestione. La gestione può fornire l'autorizzazione su base 'una tantum' se soggetta a riesame periodico.
I computer portatili devono avere una protezione dell'accesso appropriata, ad esempio, password e crittografia e non devono essere lasciati incustoditi in luoghi pubblici.
Le apparecchiature informatiche sono vulnerabili al furto, alla perdita o all'accesso non autorizzato. Mettere al sicuro computer e apparecchiature portatili quando si lasciano incustoditi.
Quando si viaggia, a causa dell'alta incidenza di furti d'auto, è inopportuno lasciarli in auto o portarli in zone pericolose.
Per preservare l'integrità dei dati, devono essere effettuati trasferimenti frequenti tra le unità portatili e il sistema principale. È necessario effettuare regolarmente la manutenzione dell'unità portatile e ricaricare regolarmente le batterie.

Gli utenti di apparecchiature informatiche portatili sono responsabili della sicurezza dell'hardware e delle informazioni in esso contenute in ogni momento, all'interno o all'esterno della proprietà
STRATESIS. L'apparecchiatura deve essere utilizzata solo dal personale STRATESIS a cui è stata rilasciata.
Tutte le dichiarazioni della politica riguardanti l'uso di software di qualsiasi natura sono valide allo stesso modo per gli utenti di apparecchiature portatili appartenenti a STRATESIS.
Gli utenti di queste apparecchiature devono prestare particolare attenzione alla protezione dei dati personali e dei dati commercialmente sensibili. L'uso di una password per iniziare a lavorare con il computer quando è acceso è obbligatoria e tutti i file sensibili devono essere almeno protetti da password, se la crittografia dei dati non è tecnicamente possibile. Ciascun computer consegnato a operatori ha due accessi utente, uno in uso all'operatore e uno la cui password è conosciuta solo dall'amministratore di sistema. Questo secondo utente ha l'accesso amministratore alla macchina.

### *4.3. Supporti rimovibili (A.8.3.1)*
I supporti rimovibili qualora contenenti informazioni aziendali non devono essere portati fuori sede dal personale senza l'autorizzazione di gestione. La gestione può fornire l'autorizzazione su base 'una tantum' se soggetta a riesame periodico.

### *4.4. Documentazione di sistema*
Tutti i sistemi devono essere adeguatamente documentati dal responsabile di progetti o servizi e devono essere tenuti aggiornati in modo che corrispondano allo stato del sistema in ogni momento.
La documentazione di sistema, compresi i manuali, deve essere protetta fisicamente (ad esempio, deve essere tenuta sotto chiave) quando non in uso.
La distribuzione della documentazione di sistema deve essere autorizzata formalmente dal gestore.

## 5. Protezione di software e informazioni

### *5.1. Software concesso in licenza*
Tutti gli utenti devono assicurarsi che vengano utilizzate solo le copie con licenza di software commerciale. È reato fare uso di copie non autorizzate di software commerciale e i trasgressori saranno passibili di provvedimenti disciplinari.
**Il caricamento e l'utilizzo di software senza licenza su apparecchiature informatiche STRATESIS non è consentito.**
Tutto il personale deve attenersi al Copyright Design and Patents Act (Decreto in materia di Diritto d'autore, Progetti e Brevetti). Secondo questo decreto è illegale copiare e utilizzare il software senza il consenso del proprietario del diritto d'autore o la licenza appropriata che dimostri che il software è stato acquistato legalmente.
Non è consentito installare software aziendali su computer privati. STRATESIS controlla l'installazione e l'utilizzo di software mediante controlli software regolari. Eventuali violazioni del diritto d'autore del software possono dar luogo a controversie personali da parte dell'autore del software o distributore e possono essere la base per un'azione disciplinare nell'ambito della politica disciplinare.

### *5.2. Software non autorizzato*
STRATESIS consente che solo il software autorizzato venga installato sui propri PC. STRATESIS richiede l'uso di specifici pacchetti di uso generale (ad esempio, elaborazione di testi, fogli di calcolo, client di posta elettronica) per facilitare la mobilità del supporto e del personale. I pacchetti non approvati non saranno supportati dal reparto di Infrastruttura Tecnologica. I pacchetti software devono rispettare e non compromettere gli standard di sicurezza STRATESIS. I giochi per computer non devono essere installati su workstation STRATESIS.

### *5.3. Controllo di virus*
STRATESIS cerca di ridurre il rischio di virus informatici attraverso l'educazione, le procedure di buona prassi e i software antivirus. Su ciascuna workstation e su ciascun server deve essere installato un software antivirus che garantisca il controllo e consenta la verifica dei file. Questo software viene aggiornato e scaricato automaticamente sulle singole workstation.

In nessun caso un utente deve disattivare o eliminare il software antivirus su un computer. Non è consentito caricare nessun supporto acquistato di recente (minidischi, CD-ROM, DVD, schede di memoria USB) da una qualsiasi fonte, a meno che non siano stati precedentemente controllati i virus mediante un pacchetto di controllo antivirus installato in locale. Gli utenti devono essere consapevoli del rischio di virus provenienti da Internet, tra cui e-mail. In caso di dubbio su eventuali dati ricevuti si prega di contattare il reparto di Infrastruttura Tecnologica per suggerimenti su antivirus.

### *5.4. Accesso alle informazioni (A.11.2.8 - A.11.2.9)*

I terminali inattivi devono essere impostati in modo da andare in timeout dopo un periodo prestabilito di inattività (sono consigliati 10 minuti). La funzionalità di timeout deve rendere intelligibili i dati sullo schermo. Nelle zone ad alto rischio, la funzionalità di timeout deve anche chiudere le sessioni applicative e di rete.
Gli utenti devono bloccare o spegnere dispositivi quando li lasciano incustoditi. Per le applicazioni ad alto rischio, deve essere considerato il limite di durata della connessione. Limitare il periodo durante il quale è consentita la connessione del terminale ai servizi informatici riduce le opportunità di accesso non autorizzato.
STRATESIS crede fortemente in una "politica della scrivania pulita". I documenti riservati non devono mai essere lasciati a portata di mano sulla scrivania dei dipendenti. Tutta la documentazione interna e dei clienti deve essere trattata come documentazione riservata.
Tutte le e-mail inviate dai dipendenti STRATESIS devono avere una firma standard in cui si afferma che la e-mail e gli eventuali file trasmessi con essa sono riservati e sono destinati esclusivamente per l'uso del singolo o dell'ente a cui sono indirizzati.

## 6. Gestione degli assets (hardware) (A.8.1.2-3 e A.8.2.3)

### *6.1. Archivio hardware*

Presso STRATESIS, viene gestito e costantemente mantenuto un inventario di tutti i computer e le apparecchiature. Il responsabile IT ha il compito di censire e tenere traccia di ogni singola attrezzatura relativa alle apparecchiature in uso e in dotazione ai singoli operatori acquistate o smaltite. Il reparto IT manterrà una copia dell'inventario ed effettuerà periodicamente una verifica.

### *6.2. Libreria software*

Tutti i software e gli strumenti sono selezionati dal reparto di Infrastruttura Tecnologica che ne detiene il registro con lo scopo di mantenere l'elenco dei software approvati e la funzione di utilizzo. Tutti i dipendenti e collaboratori possono consultare tale elenco per la determinazione del software/servizio più attinente alla lavorazione che devono svolgere. Tutti i software non presenti nell'elenco sono da intendersi come non autorizzati.

I dirigenti hanno la responsabilità di informare il reparto di Infrastruttura Tecnologica dell'acquisto di qualsiasi software. Il reparto di Infrastruttura Tecnologica mantiene una copia dell'inventario ed effettuerà periodicamente una verifica del software installato.

## 7. Continuità

### *7.1. Backup*

I dati devono essere mantenuti su una directory di rete, ove possibile, al fine di garantire l'acquisizione dei dati mediante processi di backup di routine. Se le informazioni si trovano sul disco rigido di una workstation, l'utente della workstation è responsabile del backup. Si consiglia di mantenere il backup in un'ubicazione fisica diversa (ad esempio, un computer o un disco rigido diverso) da quello dei dati di cui è stato eseguito il backup.

I dati devono essere protetti mediante procedure di backup chiaramente definite e controllate che generano dati per scopi di archiviazione e recupero di emergenza.

Il reparto di Infrastruttura Tecnologica e tutti gli altri dirigenti devono produrre istruzioni di backup scritte per ogni sistema sotto la loro gestione. Le copie di backup devono essere chiaramente etichettate e tenute in un'area sicura. Le procedure devono essere poste in atto per ripristinare il sistema ad un punto utilizzabile dal backup. Viene applicato un sistema ciclico di backup e vengono mantenute diverse generazioni di backup.

Ai dati archiviati e di ripristino deve essere attribuita la stessa sicurezza dei dati in tempo reale e almeno una copia deve essere conservata separatamente in un luogo fuori sede. I dati archiviati sono informazioni che non sono più in uso corrente, ma possono essere richieste in futuro, ad esempio, per motivi legali o scopi di controllo. I dati di ripristino devono essere sufficienti a garantire un livello di assistenza e tempi di recupero adeguati in caso di emergenza e devono essere verificati regolarmente.

Per garantire che, in caso di emergenza, i dati di backup siano sufficienti e accurati, devono essere controllati regolarmente. Questa operazione può essere eseguita automaticamente confrontando tali dati con i dati in tempo reale subito dopo il backup e utilizzando i dati di backup in test regolari del piano di emergenza.

I dati di ripristino devono essere utilizzati solo con l'autorizzazione formale del proprietario dei dati. Se i dati in tempo reale sono danneggiati, i relativi software, hardware e servizi di comunicazione devono essere controllati prima di utilizzare i dati di backup. Questo per garantire che, oltre ai dati in tempo reale, non siano danneggiati anche i dati di backup.

Tutti i dati vengono salvati, e trasferiti ogni settimana in altro locale differente dalla sede operativa di Stratesis su servizio in cloud (Microsoft Sharepoint).

### *7.2. Ripristino*

Le modalità di ripristino vengono applicate per i seguenti motivi:

- Ripristino da gravi danni per l'installazione
- Ripristino da perdita causata da danneggiamento dei dati o violazione della sicurezza
- Ripristino da danni.

Come qualsiasi altra organizzazione, STRATESIS potrebbe essere suscettibile a perdite o danni dovuti a calamità ambientali e minacce esterne (come terremoti, alluvioni e così via) che sono fuori del controllo di qualsiasi organizzazione. Nonostante non sia possibile prevedere eventi di questo tipo, STRATESIS ha adottato misure per limitarne l'impatto, stabilendo l'ubicazione principale e di backup dei sistemi centrali su infrastrutture cloud presso fornitori certificati che garantiscono un alto livello di gestione grazie all'adozione di politiche di disaster recovery e adottando misure per limitarne l'impatto, stabilendo l'ubicazione principale e di backup dei sistemi centrali in due sedi distinte tra loro.

#### 7.2.1. Perdita di alimentazione

Per la rete interna, tutti i server sono dotati di gruppi di continuità, al fine di garantire che non ci sarebbe alcuna perdita di dati prima dello spegnimento dei sistemi. Il servizio completo sarà reso disponibile dopo la ripresa dell'alimentazione.

#### 7.2.2. Server di rete

I server dove risiedono i dati sono erogati in modalità Cloud / IAAS ed i rispettivi fornitori offrono un alto grado di sicurezza:

- **Microsoft 365** risulta certificato: ISO/IEC 270001,
- **Aruba Cloud** risulta certificato: ISO 27001

### *7.3. Apparecchiature, supporti e smaltimento di dati (A.8.3.2)*

Se una macchina è sempre stata utilizzata per elaborare i dati personali, come definito ai sensi della legge sulla protezione dei dati o altri dati riservati, qualsiasi supporto di memorizzazione deve essere smaltito solo dopo che sono state utilizzate precauzioni affidabili per distruggere i dati.

Molti pacchetti software presentano routine al loro interno che scrivono i dati in file temporanei sul disco rigido. Gli utenti sono spesso inconsapevoli che questa attività è in corso e possono non rendersi conto che dati potenzialmente sensibili vengono memorizzati automaticamente sul proprio disco rigido.
Anche se il software di solito (ma non sempre) elimina questi file dopo che hanno assolto la loro funzione, i file potrebbero essere ripristinati e recuperati facilmente dal disco utilizzando il software di utilità comunemente disponibile.
Pertanto, lo smaltimento deve essere organizzato solo attraverso il reparto di Infrastruttura Tecnologica, che farà in modo che i dischi vengano cancellati secondo gli standard di sicurezza.

## 8. Politica desktop

### *8.1. Politica hardware per computer desktop*

#### 8.1.1. Scopo e ambito della politica

Questa politica specifica nei dettagli quali piattaforme hardware sono utilizzate come standard per i computer desktop STRATESIS e il livello di supporto previsto dal reparto di Infrastruttura Tecnologica.
La politica identifica e definisce:

- Le piattaforme hardware per computer desktop supportate centralmente
- Il livello di supporto che sarà fornito dal reparto di Infrastruttura Tecnologica
- I suggerimenti relativi all'hardware per i centri di sviluppo
- Le eccezioni alla politica.

#### 8.1.2. Monitoraggio e riesame delle politiche

Il reparto di Infrastruttura Tecnologica è responsabile dell'attuazione di questa politica e del suo sviluppo futuro.
Il reparto di Infrastruttura Tecnologica effettua una revisione importante delle piattaforme hardware periodicamente. Eventuali revisioni proposte della politica sono discusse con la Direzione di STRATESIS.

#### 8.1.3. La politica

##### *8.1.3.1. Piattaforma hardware e specifiche*

La piattaforma hardware per computer desktop standard STRATESIS, tra cui PC laptop/notebook, è un PC che esegue il sistema operativo desktop standard STRATESIS.
Il reparto di Infrastruttura Tecnologica fornisce una specifica di sistema minima per i PC desktop e laptop/notebook di proprietà di STRATESIS.
Tutti i computer desktop e laptop di proprietà di STRATESIS acquistati da STRATESIS per l'uso da parte del personale devono rispettare le specifiche definite.
Il responsabile del reparto deve approvare eventuali eccezioni ed essere consapevole che non ci sarà alcun supporto centrale garantito per tali eccezioni. I centri di sviluppo che introducono computer desktop classificati come eccezioni a questa politica devono verificare con il reparto di Infrastruttura Tecnologica che tali sistemi funzionino in modo efficace, senza apportare alcuna modifica all'infrastruttura corrente o avere un impatto negativo sul computer e la rete di sicurezza STRATESIS.

##### *8.1.3.2. Supporto*

Il supporto per il servizio IT per la piattaforma hardware desktop standard è fornito come segue:

| Livello di supporto | Definizione | Ciclo di vita dei PC |
|---|---|---|
| Supporto completo | Supporto completo per consentire quanto segue:<br>●Connessione alla rete di dati STRATESIS<br>●Funzionamento efficace del software desktop standard STRATESIS | Anni 1-3 dopo l'acquisto |

| | | |
|---|---|---|
| | • Funzionamento efficace e corretto di tutto il software supportato nelle categorie Standard Office IT e infrastructure Tools<br>Queste categorie di software includono il software IT per ufficio di base e il software antivirus installati sui desktop di proprietà di STRATESIS. | |
| Supporto parziale | Alcune applicazioni potrebbero essere eseguite lentamente (nonostante funzionino ancora correttamente) e potrebbe essere richiesto un aggiornamento hardware a medio termine (ad esempio, più memoria).<br>Eccezione - Alcune nuove periferiche potrebbero non funzionare se utilizzano schede di interfaccia che non sono disponibili per i sistemi più vecchi. | Anni 4-5 |

L'obiettivo di STRATESIS è quello di sostituire i PC secondo un ciclo quinquennale, con adeguata migrazione di apparecchiature tra utenti e centri di sviluppo, al fine di raggiungere questo obiettivo. Anche se alcuni PC desktop più vecchi di 5 anni possono ancora connettersi alla rete di dati STRATESIS senza problemi e funzionare in modo soddisfacente, va riconosciuto che ciò non può essere garantito e il reparto di Infrastruttura Tecnologica non offrirà un supporto significativo per risolvere i problemi relativi a tali apparecchiature.

I centri di sviluppo devono essere consapevoli del rischio e del costo maggiore che implica il supporto di PC più vecchi di 5 anni e devono pianificare programmi di sostituzione IT per tali apparecchiature.

Il supporto del reparto di Infrastruttura Tecnologica o la fornitura di servizi per computer desktop di proprietà di STRATESIS diversi dalla piattaforma hardware per desktop standard non sono garantiti.

Tuttavia, qualora il reparto di Infrastruttura Tecnologica venisse a conoscenza di poter fornire supporto nella risoluzione dei problemi con altre piattaforme hardware, condividerà questa informazione con il personale.

Il reparto di Infrastruttura Tecnologica fornisce supporto per il collegamento di periferiche di uso comune connesse alla piattaforma hardware desktop standard, fornendo i driver software per le periferiche disponibili per il sistema operativo desktop standard.

Tale supporto include la risoluzione dei problemi per le stampanti desktop consigliate dal reparto di Infrastruttura Tecnologica dai fornitori approvati

Per le altre periferiche di uso comune come scanner, fotocamere digitali e PDA, il reparto di Infrastruttura Tecnologica fornisce consulenza di base per assistere nell'approvvigionamento e per garantire che tali periferiche funzionino in modo efficace con la piattaforma hardware desktop standard, con il software standard STRATESIS e, dove applicabile, con i servizi centrali come e-mail. Tale consulenza varierà a seconda delle necessità, delle norme in via di sviluppo e del mercato.

#### *8.1.3.3. Approvvigionamento e distribuzione*

Il reparto di Infrastruttura Tecnologica fornisce consulenza di acquisto per la piattaforma hardware desktop standard, inclusi specifiche minime e modelli standard di fornitori STRATESIS approvati e stampanti desktop consigliate.
Il reparto di Infrastruttura Tecnologica fornisce supporto e formazione per la distribuzione di software su piattaforma hardware desktop standard.
I PC più vecchi di 5 anni devono essere smaltiti in conformità con la politica STRATESIS e le normative locali.

### *8.2. Politica software per computer desktop*

#### 8.2.1. Scopo e ambito della politica

Questa politica illustra nei dettagli come i sistemi operativi e altro software presenti sui computer desktop STRATESIS vengono distribuiti e supportati dal reparto di Infrastruttura Tecnologica. Vengono anche forniti suggerimenti sulle migliori pratiche per assistere i centri di sviluppo nella distribuzione e nella creazione di un'interfaccia con i servizi centrali. I centri di sviluppo sono tenuti a rispettare queste politiche e questi suggerimenti, ma sono previste disposizioni per eccezioni giustificabili.
La politica identifica e definisce:

- I sistemi operativi supportati a livello centrale
- Il software applicativo supportato a livello centrale
- Le possibili eccezioni alla politica.

#### 8.2.2. Monitoraggio e riesame delle politiche

Il reparto di Infrastruttura Tecnologica è infine responsabile dell'attuazione di questa politica e del suo sviluppo futuro. Un riesame completo viene eseguito per determinare il software successivo supportato con cadenza annuale.

#### 8.2.3. La politica

##### *8.2.3.1. Sistemi operativi supportati*

Un sistema operativo desktop standard viene utilizzato per i computer desktop STRATESIS per i quali il reparto di Infrastruttura Tecnologica garantisce il supporto. Questo sistema operativo è il sistema operativo predefinito installato su tutti i sistemi di computer desktop del personale acquistati da STRATESIS.

*Eccezioni*

- Sistemi di computer desktop diversi, in cui lo sviluppo non può essere effettuato in modo pratico utilizzando un PC. Sono incluse le workstation basate su Macintosh e UNIX.
- PC desktop dove lo sviluppo non può essere effettuato in modo pratico utilizzando il sistema operativo desktop del standard. Sono inclusi ad esempio i PC necessari per eseguire software di applicazioni che non funzionano correttamente con il sistema operativo desktop standard.
- Computer desktop collegati ad apparecchiature specifiche, laddove il fornitore delle apparecchiature insiste su un particolare sistema operativo diverso dal sistema operativo desktop standard.

Il responsabile del reparto deve approvare eventuali eccezioni ed essere consapevole che non ci sarà alcun supporto centrale garantito per tali eccezioni.
Supporto completo per il sistema operativo desktop standard è fornito dal reparto di Infrastruttura Tecnologica, incluso il supporto helpdesk e il follow-up tecnico di secondo livello dei problemi.
È fornito anche il supporto per il predecessore del sistema operativo desktop standard, ma nessun lavoro di sviluppo è effettuato utilizzando questo sistema operativo, a meno che non sia assolutamente essenziale per il mantenimento di programmi strategici. Il supporto per il predecessore è gradualmente eliminato durante il ciclo di vita del sistema operativo standard corrente, in modo che in un punto unico nel tempo ci siano solo due sistemi operativi desktop che ricevono il supporto dal reparto di Infrastruttura Tecnologica.
Ove richiesto per lo sviluppo, viene fornito un determinato supporto per garantire che applicazioni Linux possano coesistere e funzionare su PC insieme al sistema operativo desktop standard.
Il reparto di Infrastruttura Tecnologica fornisce un servizio centrale per assicurare che il sistema operativo desktop standard possa essere corretto/aggiornato automaticamente su tutti i sistemi di proprietà di STRATESIS che sono collegati, o possono essere collegati alla rete, al fine di mantenere la sicurezza del sistema. La politica di sicurezza

del dominio corrente per aggiornare i computer sulla rete è impostata in modo tale che gli aggiornamenti vengano scaricati automaticamente, ma l'installazione deve essere eseguita manualmente dall'utente della workstation. È responsabilità dell'utente aggiornare la propria workstation in modo tempestivo. È responsabilità del reparto di Infrastruttura Tecnologica aggiornare i server su base mensile.
Il reparto di Infrastruttura Tecnologica fornisce a ciascun reparto la possibilità di installare nuove workstation da immagini software, se possibile.
É garantito che tutti i servizi forniti a livello centrale che hanno un'interfaccia client desktop (ad esempio e-mail, applicazioni web e amministrative) e software con licenza funzioneranno con il sistema operativo desktop standard.

#### 8.2.4. Software applicativo supportato

Il reparto di Infrastruttura Tecnologica fornisce il supporto completo per il software applicativo gestito/utilizzato dall'azienda.

### *8.3. Approvvigionamento di computer desktop e politica di distribuzione*

#### 8.3.1. Scopo e ambito della politica

Questa politica illustra nei dettagli l'approvvigionamento e la distribuzione dei sistemi di computer desktop STRATESIS e il livello di supporto che viene fornito per tali sistemi dai servizi centrali. Vengono anche forniti suggerimenti e linee guida sulle migliori pratiche, per assistere gli uffici STRATESIS con le strategie di approvvigionamento IT.
La politica identifica e definisce:

- La politica di STRATESIS su fornitori approvati e supporto per l'approvvigionamento centrale
- Le specifiche minime consigliate per le apparecchiature e i modelli standard
- La politica di STRATESIS in materia di sostituzione e smaltimento delle apparecchiature.

#### 8.3.2. La politica

##### *8.3.2.1. Fornitori*

L'ufficio STRATESIS è responsabile di individuare i fornitori STRATESIS approvati per computer desktop, portatili e stampanti.
L'ufficio STRATESIS controlla le prestazioni del fornitore su una base costante, secondo le modalità stabilite in ambito sistema di gestione integrato. Se le sue prestazioni sono state inaccettabili, il fornitore ne viene informato e l'ufficio STRATESIS lavorerà con il fornitore per identificare i miglioramenti che devono essere attuati al fine di raggiungere un livello accettabile di servizio. Se le prestazioni del fornitore non migliorano in modo soddisfacente, l'ufficio STRATESIS deciderà se e quando sostituire il fornitore.
Un'analisi approfondita dei fornitori è eseguita dall'ufficio STRATESIS in collaborazione con il reparto di Infrastruttura Tecnologica, quando vengono annunciati nuovi accordi per fornitori di computer desktop e portatili. In questa fase verranno confermati i fornitori attuali o verranno scelti nuovi fornitori.
L'ufficio STRATESIS garantisce che qualsiasi disposizione di acquisto di STRATESIS con i fornitori di computer desktop e portatili sia in conformità con la legislazione nazionale ed europea vigente.

##### *8.3.2.2. Specifiche minime consigliate e modelli standard*

Il reparto di Infrastruttura Tecnologica riesamina le specifiche minime consigliate e i modelli standard per computer desktop, portatili e stampanti STRATESIS.

##### *8.3.2.3. Distribuzione e smaltimento*

L'obiettivo di STRATESIS è quello di sostituire i PC secondo un ciclo quinquennale, con adeguata migrazione di apparecchiature al fine di raggiungere questo obiettivo.
Dopo cinque anni di funzionamento all'interno di STRATESIS, computer desktop, portatili e stampanti devono essere smaltiti rivolgendosi a una società di smaltimento apparecchiature IT registrata, per poter garantire la conformità con la legislazione nazionale ed europea in materia di smaltimento di apparecchiature elettriche.

## 9. Politica per la posta elettronica (A.13.2.1 - 2)

### *9.1. Accesso a e-mail aziendale*

È responsabilità degli utenti attivare la funzionalità “verifica in due passaggi”, che aumenta il livello di protezione evitando che un eventuale malintenzionato, che si è impossessato illecitamente della PW, acceda al server di posta. L’opzione è fortemente consigliata.
É possibile bypassare questa opzione inserendo il dispositivo client tra quelli autorizzati.

### *9.2. Cura nella redazione delle e-mail*

È responsabilità degli utenti redigere attentamente tutte le e-mail, tenendo conto di qualsiasi forma di discriminazione, molestia, rappresentazione di STRATESIS e diffamazione di questioni relative alla protezione dei dati. Le e-mail del personale rappresentano una forma di comunicazione aziendale e, pertanto, devono essere redatte con la stessa cura delle lettere. Prima di inviare il messaggio, provare a leggerlo per assicurarsi che sia comprensibile e appropriato. Non inviare email con contenuti sensibili o emozionali. Se si è arrabbiati, rileggere il messaggio quando si è calmi. Non redigere mai una e-mail usando esclusivamente lettere maiuscole; usare i caratteri di una frase normale. Gli utenti devono fare attenzione quando rispondono a e-mail precedentemente inviate a un gruppo **prestando attenzione ai destinatari principali ed eventualmente quelli in copia conforme se presenti**.

### *9.3. Virus e allegati*

I dipendenti sono responsabili del controllo antivirus di ogni allegato ricevuto prima dell'apertura.

### *9.4. Riservatezza delle informazioni*

Le e-mail rappresentano un metodo di comunicazione poco sicuro, con contenuti che possono essere facilmente copiati, trasmessi o archiviati. I dati sensibili non devono essere inviati tramite questo metodo.

### *9.5. Applicazione e controllo*

STRATESIS si riserva il diritto di effettuare attività di controllo sui propri sistemi, anche senza preavviso.
STRATESIS si impegna a garantire che qualsiasi controllo venga effettuato con riferimento alla privacy dell'utente e rispettando la legge sulla protezione dei dati, la legge che disciplina i poteri di indagine (RIPA), la legge sulle transazioni commerciali legittime e la legge sui diritti umani.

### *9.6. Conservazione ed eliminazione*

L'eliminazione di vecchie e-mail deve essere gestita da ogni singolo utente, tenendo in considerazione i livelli di storage, i livelli d'archiviazione, i dati contrattuali e le questioni relative agli accertamenti legali.

### *9.7. Posta indesiderata*

Le e-mail non devono essere inviate a un numero elevato di persone, a meno che non siano strettamente correlate al loro lavoro. L'invio di e-mail non richieste a molti utenti ('spamming') è uno spreco di tempo e può interrompere il servizio, a causa di ritardi nelle prestazioni, per gli altri utenti.

### *9.8. File di grandi dimensioni*

L'invio di file di grandi dimensioni via e-mail dovrebbe essere evitato per quanto possibile. Si consiglia l'uso di un software di compressione appropriato con licenza (ad esempio file * .zip). I file di grandi dimensioni (più grandi di 20 MB) devono essere inviati con metodi diversi dalle e-mail.

### *9.9. Protezione del terminale*

Se un utente lascia un terminale aperto e connesso quando si allontana dalla scrivania, un utente malintenzionato potrebbe inviare messaggi a suo nome. Assicurarsi che il terminale sia bloccato o disconnesso.

### *9.10. Tempeste di posta*

Le 'tempeste di posta", vale a dire lunghe discussioni inviate a una lista di distribuzione, devono essere evitate e deve essere utilizzata invece la comunicazione verbale.

## 10. Linee guida sugli antivirus

### *10.1. Cos'è un virus?*

Un virus è una parte dannosa di software che può essere trasferita tra programmi o tra computer a insaputa dell'utente. Quando il software virus viene attivato (mediante istruzioni integrate, ad esempio in una data particolare), esegue una serie di azioni quali la visualizzazione di un messaggio, il danneggiamento di software, file e dati per renderli inutilizzabili e l'eliminazione di file e/o dati. Nonostante molti dei virus prodotti siano benigni e non causino alcun danno reale al sistema infetto, costituiscono sempre una violazione della sicurezza. Quando un virus o un worm viene rilasciato nel dominio pubblico, worm di rete e virus mass mailer possono talvolta diffondersi a livello mondiale prima che i fornitori di antivirus abbiano il tempo di produrre aggiornamenti. Anche gli aggiornamenti antivirus giornalieri non sempre sono sufficienti a garantire la sicurezza da tutte le possibili minacce.
Un worm è un virus auto-replicante che non altera i file, ma risiede nella memoria attiva e si duplica. I worm utilizzano parti di un sistema operativo che sono automatiche e in genere invisibile all'utente. In genere i worm vengono rilevati solo quando la loro replica incontrollata consuma risorse di memoria, rallentando o arrestando le altre attività.
Nei computer, un cavallo di Troia è un programma in cui codice dannoso o nocivo è contenuto all'interno di programmazione o dati apparentemente innocui, in modo da poter ottenere il controllo ed arrecare un determinato tipo di danni.

### *10.1. Cos'è un malware?*

Nella sicurezza informatica il termine malware indica un qualsiasi software creato allo scopo di causare danni a un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato di "programma malvagio".

### *10.2. Azioni per prevenire la diffusione di virus e malware (A.11.2.1)*

Nonostante vengano prese precauzioni a livello di rete per ridurre la diffusione e l'impatto di worm e virus, non è possibile rendere il processo completamente efficace. La protezione da virus e worm non è un processo che può essere lasciato interamente agli amministratori di sistema e ai software antivirus. Il massimo sforzo di amministratori ed esperti di sicurezza non è sufficiente; tutti gli utenti di computer devono fare la loro parte adottando semplici precauzioni, come quelle descritte di seguito.

### *10.3. Prevenzione antivirus e malware implementata*

Si è deciso di installare su ogni PC o assets assegnato ai dipendenti un antivirus e malware con licenza (Norton). La licenza del SW in questione ha validità 1 anno. All'interno di quest'anno l'antivirus si aggiorna automaticamente. Allo scadere della licenza, questa viene rinnovata e l'amministratore di sistema provvede all'aggiornamento su tutte le macchine.

### *10.4. Evitare il software non autorizzato (A.9.4.4 e A.9.4.5)*

Programmi come giochi, programmi ingannevoli, screensaver divertenti, programmi di utilità non autorizzati e così via possono a volte essere fonte di difficoltà, anche se in realtà non sono dannosi. Ecco perché si consiglia vivamente di non installarli. Se si asserisce che tali programmi siano una forma di antivirus o programma di utilità anti-Trojan, esiste un rischio elevato che siano in realtà in qualche modo dannosi.

### *10.5. Trattare tutti gli allegati con cautela*

È opportuno essere cauti con gli allegati di posta elettronica provenienti da persone che non si conoscono. Tuttavia, anche se gli allegati vengono inviati da qualcuno che si conosce, è opportuno non dare per scontato che siano innocui perché ci si fida del mittente. I worm in genere vengono inviati e diffusi senza che la persona dal cui account vengono diffusi lo sappia. Se non si conosce il mittente o non si aspetta alcun messaggio da parte del

mittente su quell'argomento, è opportuno controllare con il mittente se aveva intenzione di inviare un messaggio, e in questo caso, se aveva intenzione di includere un allegato. Se si era in attesa di un allegato dal mittente, questa procedura potrebbe non essere applicabile. Tuttavia, un virus invia un'e-mail in cui viene indicato che un allegato "sicuro" è in arrivo e quindi invia l'e-mail con una copia di se stesso come allegato.
Tenere presente che gli allegati attesi e legittimi possono essere infetti da virus: worm e virus sono correlati ma causano problemi leggermente diversi.
Considerare tutto ciò che risponde ai seguenti criteri con particolare sospetto:

- Se Il messaggio è stato inviato da qualcuno che non si conosce, che non ha alcun motivo legittimo per inviarlo;
- Se un allegato arriva con un messaggio vuoto;
- Se nel messaggio è presente un testo che non menziona l'allegato;
- Se è presente un messaggio ma sembra non avere senso;
- Se è presente un messaggio, ma sembra insolito da parte del mittente (sia nel contenuto che nel modo in cui è espresso);
- Se riguarda materiale insolito;
- Se il messaggio non contiene alcun riferimento personale (ad esempio, un breve messaggio del tipo "Devi dare un'occhiata a questo", oppure "Ti mando questo messaggio perché ho bisogno del tuo consiglio" o "ti amo!");
- Se l'allegato ha un'estensione di nome file che indica un file di programma o un file di dati che può contenere programmi eseguibili sotto forma di macro (.BAT, .CHM, .CMD, .COM,
- .DLL, .DOC, .DOT, .EXE, .FON, .HTA, .JS, .OVL, .PIF, .SCR, .SHB, .SHS, .VBS, .VBA, .WIZ, .XLA,
- .XLS …);
- Se ha un nome di file con una "doppia estensione", come FILENAME.JPG.vbs o FILENAME.TXT.scr, che può essere estremamente sospettosa. Per quanto riguarda Windows, è l'ultima parte del nome che conta; controllare quindi l'allegato in base all'elenco sopra riportato per scoprire se si tratta di un programma come quelli elencati, mascherato da file di dati, ad esempio un file di testo o un file JPEG (grafico).

In tutti i casi di cui sopra, si consiglia di controllare con il mittente che abbia deliberatamente inviato la mail o l'allegato in questione.

### 10.5.1. Evitare macro non necessarie

Se Word o Excel avvisano che un documento che si sta per aprire contiene macro, considerare il documento con particolare sospetto, a meno che non si aspetti il documento e non sia previsto che contenga macro. Anche in questo caso, non attivare le macro se non è necessario. Può valere la pena verificare con la persona che ha inviato il messaggio se si prevedeva che contenesse macro.

### 10.5.2. Essere prudenti con i file crittografati

Se si riceve un allegato crittografato o un allegato protetto da password, si tratterrà in genere di posta legittima da parte di qualcuno che si conosce, inviata intenzionalmente (sebbene è improbabile che il mittente lo sappia, nel caso in cui contenga un virus). Tuttavia, ciò non significa necessariamente che l'allegato non contenga un virus. Se l'allegato è infetto, la crittografia non è in grado di correggerlo. Inoltre, gli allegati crittografati in genere non possono essere sottoposti a scansione alla ricerca di virus in transito; è responsabilità del destinatario assicurarsi che il file decrittografato venga controllato prima di essere aperto.

### 10.5.3. Segnalare il problema

Se si pensa di aver ricevuto un virus/malware, segnalare il problema immediatamente al reparto IT, non aprire file sospetti, attendere l'intervento IT.