# Procedura generale 5.2

## Protezione dei dati

**Identificazione**

| | | | |
|---|---|---|---|
| Nome file | GFC PG 5.2 R0 Protezione dei dati.docx | | |
| Tipo | Documento Qualità | | |
| Visibilità | ☐ Riservato | ☑ Interno | ☐ Pubblico |
| Stato | ☑ In lavorazione | ☐ Bozza | ☐ Pubblicato |

**Approvazione**

| Rev | Data | Motivo e descrizione della modifica | Redatta | Verificata | Approvata |
|---|---|---|---|---|---|
| 0 | 05/06/2020 | Introduzione della procedura di gestione dei documenti | | | |

**Riservatezza**

Questo è un documento riservato. Secondo gli standard di condotta aziendale, questo documento non può essere condiviso al di fuori dell'Organizzazione, ma può essere pubblicato sulla rete dell'Organizzazione senza ulteriori restrizioni.
Questo documento può essere condiviso con il cliente o con altre parti interessate, se esiste un accordo adeguato.

**Dichiarazione di conformità**

Questo documento è stato redatto in conformità allo standard ISO 9001

# Sommario

# 0 PREMESSA -Dichiarazione sulla politica di sicurezza delle informazioni

La direzione dell'Organizzazione si impegna a trasmettere e a fare applicare ai propri dipendenti la politica sulla sicurezza delle informazioni con lo scopo di proteggere le informazioni e i dati dell'Organizzazione, dei suoi dipendenti, clienti, fornitori e di altri parti interessate da tutte le minacce, interne o esterne, intenzionali o accidentali.
L'intento dell'Organizzazione è, in particolare, di garantire che:

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

È compito diretto del **Titolare dei Dati** garantire le idonee risorse economiche, infrastrutturali e umane per il mantenimento della politica di sicurezza delle informazioni.
Il Responsabile della Protezione dei Dati dell'organizzazione:

9. analizza il rischio e pianifica la politica,
10. promuove e fornisce consigli e indicazioni per l'attuazione delle migliori prassi e per l'adozione di idonei comportamenti dei dipendenti al fine di ridurre al minimo il rischio
11. effettua il controllo ed il monitoraggio della sua implementazione
12. propone le azioni correttive e di miglioramento,

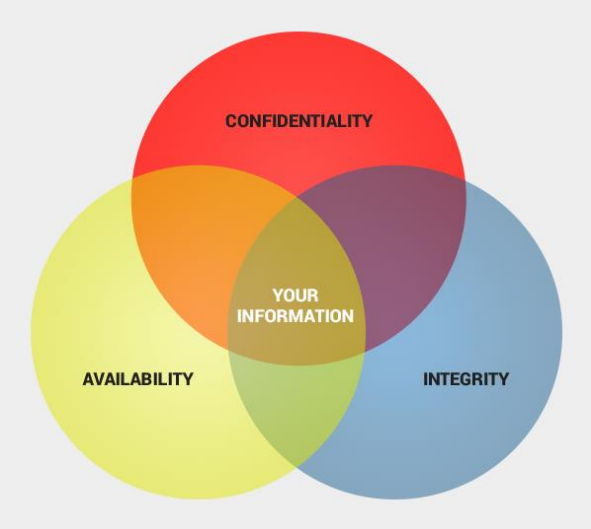
Tutti i **Responsabili del Trattamento dei Dati** sono direttamente responsabili dell'attuazione della politica all'interno delle proprie aree di competenza e della osservanza della politica medesima da parte dei **Soggetti Autorizzati** al trattamento dei dati.
**L'incaricato IT** è il soggetto (singolo o in team) incaricato dell'**information technology (IT)** service management (o gestione dei servizi IT, abbreviato in ITSM) e si occupa di pianificare, progettare, gestire e manutenzionare, anche affidando a terzi specializzati, i sistemi IT di un'organizzazione.

# 1 Introduzione

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

## 1.1 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.




### 1.1.1 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.

### 1.1.2 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.

### 1.1.3 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.

## 1.2 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.

### 1.2.1 Tutela dei dati personali sensibili

Chiunque elabori o utilizzi le informazioni personali deve rispettare i seguenti principi come definiti nella normativa di riferimento (regolamento UE 2016/679).
I dati personali devono essere:

1. Trattati in modo corretto e lecito
2. Ottenuti per finalità determinate e legittime e trattati solo in conformità con la notifica al Garante
3. Adeguati, pertinenti e non eccessivi
4. Accurati e, se necessario, aggiornatiConservati per il tempo strettamente necessario
5. Trattati in conformità con i diritti dei singoli
6. 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.

### 1.2.2 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.

### 1.2.3 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.

### 1.2.4 Sistema di gestione per la sicurezza delle informazioni

La ISO 27001 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.
L'organizzazione ha implementato un sistema di gestione per la sicurezza delle informazioni conforme a tale schema.

## 1.3 Necessità di una politica di sicurezza delle informazioni

I dati memorizzati nei sistemi utilizzati dall'Organizzazione 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 dell'Organizzazione delle azioni consentite e vietate per evitare eventuali incomprensioni e controversie future, correlate in particolare a richieste da parti esterne.
La sicurezza delle informazioni nell'Organizzazione 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.

## 1.4 Obiettivi della politica di sicurezza

Gli obiettivi della politica di sicurezza delle informazioni sono:

1. 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
2. Garantire che tutti gli appaltatori e i loro dipendenti abbiano una giusta consapevolezza e preoccupazione per la sicurezza delle informazioni dell'Organizzazione;
3. Fornire un quadro contenente i concetti per stabilire standard, procedure e strutture informatiche per l'implementazione della sicurezza dei sistemi informatici;
4. Soddisfare gli obiettivi generali per la sicurezza dei sistemi informatici contenuti nella norma ISO 27001
5. Specificare le responsabilità dell'Organizzazione;

6. Garantire che tutto il personale abbia consapevolezza della legge sulla protezione dei dati e delle sue implicazioni;
7. Garantire che tutto il personale abbia consapevolezza della legge sull'uso improprio del computer;
8. 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.

## 1.5 Quali sono i soggetti interessati dalla politica

La politica si applica a tutti i dipendenti dell'Organizzazione. Si applica anche agli appaltatori e ai visitatori, non dipendenti dell'Organizzazione, ma che sono impegnati a lavorare con l'Organizzazione o che hanno accesso a informazioni dell'Organizzazione.
La politica si applica a tutti i luoghi da cui si accede ai sistemi dell'Organizzazione (compreso l'uso domestico o altri usi remoti). Laddove sono presenti collegamenti che consentono alle altre organizzazioni di avere accesso alle informazioni dell'Organizzazione, l'Organizzazione stessa verifica 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 dell'Organizzazione è più severa, i dipendenti dell'Organizzazione che lavorano per quel cliente si atterranno a tali regole più severe.
La politica si applica a tutti i sistemi e tutte le informazioni.

## 1.6 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:

1. Lavoro di sviluppo e comunicazione ad esso associata
2. Ricerca
3. Sviluppo educativo personale
4. Amministrazione e gestione
5. Attività di consulenza per L'Organizzazione
6. Corrispondenza personale, laddove non connesso ad alcuna attività commerciale,

La politica dell'Organizzazione prevede che tutto l'uso delle strutture debba essere lecito, onesto e decoroso e tenere conto dei diritti e della sensibilità di altre persone.

## 1.7 Riesame e controllo

È compito del responsabile della Protezione dei Dati eseguire il riesame periodico della politica alla luce delle circostanze mutevoli. Il riesame viene effettuato ogni anno o quando si verificano modifiche significative.
Esistenza e modifiche della politica saranno comunicati a tutti i dipendenti attraverso i canali regolari, mentre la sensibilizzazione viene aumentata mediante l'approvazione obbligatoria da parte di ciascun dipendente.

# 2 Accesso alla rete

## 2.1 Accesso ai sistemi

Il personale dell'Organizzazione e i dipendenti esterni accedono solo ai sistemi per cui sono autorizzati. E' 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 contengono 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.

## 2.2 Registrazione di utenti

Procedure formali vengono utilizzate per controllare l'accesso ai sistemi.
Un Responsabile del Trattamento dei Dati può approvare la richiesta di accesso e autorizzare l'incaricato IT all'apertura del nuovo account utente.
Il livello di accesso è determinato 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, su richiesta del Responsabile del Trattamento dei Dati.
Gli ospiti possono accedere solo alla rete a loro dedicata che non consente l'accesso a nessun dato aziendale né al repository ma solo l'accesso a internet.
I dipendenti invece possono accedere alla rete Dati invece, che consente l'accesso al repository aziendale e ai dati dopo aver richiesto la registrazione al Responsabile del Trattamento.

### 2.2.1 Procedura di registrazione alla rete Dati

Dopo aver fatto la richiesta di accesso alla rete Dati al Responsabile del Trattamento dei Dati, quest'ultimo procede all'inserimento di una chiave di protezione sul client del dipendente e alla configurazione lato firewall di una autorizzazione.

## 2.3 Gestione utente/password

Il nome utente o username è uno pseudonimo utilizzato da un utente per farsi identificare da un sistema operativo, da un elaboratore o da un servizio online. Il nome utente può essere deciso dal Responsabile del Trattamento dei Dati, dall'incaricato IT o dallo stesso utente. Nel caso in cui la conferma dello pseudonimo avvenga via posta elettronica può essere utilizzato anche lo stesso account dell'utente.
Una password è un' "informazione di autenticazione riservata costituita da una stringa di caratteri" utilizzata per accedere ai sistemi informatici. La prima password può essere decisa dal Responsabile del Trattamento dei Dati, dall'incaricato IT o dallo stesso utente. La password viene cambiata dopo il primo accesso, in maniera che l'incaricato IT non ne mantenga la conoscenza. Le password sono mantenute riservate sotto la responsabilità dei singoli utenti e non sono utilizzate da nessun altro nemmeno per un breve periodo di tempo.
L'utente garantisce che la password non sia facilmente "individuabile", non sia scritta su nessun documento accessibile e che, se del caso, segua le indicazioni riportate in una istruzione (*) emessa dal Responsabile del Trattamento dei Dati.
E' prevista, in caso di smarrimento, una modalità per il recupero di username e password.
Fornire una password autorizzata a una persona non autorizzata al fine di ottenere l'accesso a un sistema informatico è un illecito disciplinare.
È buona norma utilizzare username e password per gli 'screensaver' in uffici con più occupanti ed essenziale nelle aree comuni.
Il Responsabile del Trattamento dei Dati è autorizzato alla elaborazione e al mantenimento di un elenco delle credenziali di accesso degli utenti agli asset utilizzati per il recupero delle stesse in caso di smarrimento.
Il controllo degli account dell'Organizzazione, dei diritti di accesso e delle autorizzazioni (Active Directory) viene effettuato in fase di riesame almeno una volte l'anno o a richiesta.
*(*) Per es: Le password sono conformi ai requisiti di complessità. Esse contengono almeno 8 caratteri di cui almeno un carattere maiuscolo, uno minuscolo, un carattere non alfabetico e una cifra (da 0 a 9).*

## 2.4 Lavoro a domicilio o telelavoro

L'accesso a Internet comporta un rischio per la sicurezza, in quanto è possibile scaricare virus o programmi in grado di effettuare ricerche nella rete e infiltrarsi in sistemi di sicurezza delle password. È necessario quindi fare attenzione durante il trasferimento dei dati tra il PC di casa e la rete dell'Organizzazione. L'utilizzo di PC personali è assolutamente sconsigliato e vietato se non in casi di particolare urgenza. Nel caso dell'utilizzo di PC di casa utilizzati per la manipolazione dei dati dell'Organizzazione questi devono avere un software antivirus aggiornato, mentre i dati in sé devono essere crittografati quando utilizzati al di fuori della rete dell'Organizzazione.
Il collegamento da casa (o dall'esterno) alla rete aziendale è possibile solo mediante canale VPN sicuro. L'accesso VPN è concesso dall'incaricato IT sulla necessità di avere una base, su previa approvazione del Responsabile del Trattamento dei Dati. 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 Abaco o se non è più necessario.
L'accesso dall'esterno in RDP avviene tramite autenticazione VPN e con l'uso del servizio disponibile dal sistema operativo configurato con l'autenticazione client-server.
E' possibile organizzare telelavoro con sistemi di gestione dei dati esterni al sistema informativo aziendale gestito su server. In questo caso i dati personali devono essere completamente esclusi, oscurati o coperti da pseudonimizzazione.

### 2.4.1 Trasporto di hardware, dati e documenti riservati

I dipendenti operano, con ragionevole cura, per ridurre al minimo il rischio di furto o danneggiamento di hardware, dati e documenti riservati durante il trasporto.
L'apparecchiatura IT viene conservata in un ambiente pulito e sicuro.
Durante il trasferimento dell'apparecchiatura tra casa e luogo di lavoro, i dipendenti non lasciano mai incustodita l'apparecchiatura. Nessun dispositivo HW aziendale viene lasciato in auto durante la notte.

### 2.4.2 Conservazione

I dipendenti che lavorano da casa adottano tutte le misure ragionevoli per ridurre al minimo la visibilità dei computer da fuori casa e chiudono 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.

## 2.5 Personale che lascia l'impiego

Prima che un dipendente lasci l'impiego o cambi mansioni, il Responsabile del Trattamento dei Dati deve assicurarsi che:

1. Il dipendente venga informato per iscritto che continua ad essere vincolato dall'accordo di riservatezza firmato
2. Tutti gli account e le password vengano rimossi o modificati per negare l'accesso
3. 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
4. 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
5. 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
6. Le proprietà del reparto vengano restituite
7. 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.
L'incaricato IT eliminerà o disabiliterà, nel loro ultimo giorno di lavoro, tutti i codici identificativi e le password dei membri del personale che lasciano l'impiego nell'Organizzazione. Prima che il membro del personale lasci l'impiego, il responsabile del trattamento dei dati garantisce che tutti i file di continuo interesse per l'attività dell'Organizzazione vengano trasferiti ad un altro utente.
In alcuni casi in cui il dipendente che lascia l'impiego conserva un rapporto formale con l'Organizzazione, a tale dipendente può essere consentito l'accesso agli account dell'Organizzazione dopo che ha lasciato l'impiego, per un periodo limitato di tempo.

## 2.6 Sicurezza di accesso di terzi

Tutti i visitatori devono avere un documento di identificazione ufficiale rilasciato dall'Organizzazione(badge visitatori) e gli orari di arrivo e di partenza devono essere registrati sull'apposito registro presente alla reception aziendale. Se devono essere emesse password temporanee per consentire l'accesso a sistemi riservati, tali password devono essere disattivate quando il visitatore esce dal sistema. 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 assistenza IT quando il personale temporaneo lascia l'impiego.
Il reparto di assistenza IT deve seguire la procedura per il controllo sicuro di appaltatori chiamati per la manutenzione e il supporto di apparecchiature informatiche e software. L'appaltatore può lavorare sul posto o in remoto tramite un collegamento di comunicazione (VPN). Il reparto di assistenza IT deciderà il controllo più adatto.
A nessuna parte esterna è consentito l'accesso alle reti dell'Organizzazione, a meno che l'ente non sia autorizzato formalmente. Tutte le parti esterne saranno tenute a firmare accordi di sicurezza e di riservatezza con l'Organizzazione.
L'Organizzazione controlla tutto l'accesso esterno ai propri sistemi attivando o disattivando le connessioni per ogni prescrizione di accesso autorizzato.
L'Organizzazione 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 dell'Organizzazione.

## 2.7 Audit interno

Il riesame dell'audit interno di tutti i sistemi principali e degli account utente verrà eseguito a intervalli di 1 anno. All'interno di questi riesami, tutti i controlli chiave all'interno di un sistema, compresi i controlli di computer, sono testati e rivisti. L'incaricato IT ha il compito di esercitare controlli adeguati e le modalità di controllo interno si applicano a tutti i sistemi.

## 2.8 Sicurezza della rete

È compito dell'incaricato IT garantire che i diritti di accesso e il controllo del traffico su tutte le reti dell'Organizzazione siano mantenuti correttamente.
L'accesso ai sistemi è controllato su due livelli:

1. Attraverso le regole di firewall e proxy
2. Attraverso gruppi di dominio e politiche in Active Directory.

Rientra nella politica e nella pratica dell'Organizzazione consentire l'accesso a tutte le informazioni sensibili solo attraverso protocolli di rete sicuri (ad esempio SSL, HTTPS, FTPS, IPsec). È vietato l'accesso esterno mediante protocolli non sicuri alla rete Abaco (ad esempio, RDC, FTP).

I dipendenti non devono impostare manualmente gli indirizzi IP sulle proprie interfacce di rete. Tali indirizzi devono essere assegnati automaticamente dal server DHCP. È necessario prestare particolare attenzione quando la macchina virtuale viene avviata, per evitare conflitti di indirizzi MAC e IP.
È compito dell'incaricato IT garantire che le comunicazioni di dati su reti remote e strutture informatiche non compromettano la sicurezza dei sistemi dell'Organizzazione.

# 3 Sicurezza hardware

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 dall'incaricato IT. Il controllo degli accessi è effettuato mediante serratura con chiave. Le apparecchiature di comunicazione sono posizionate in ambienti dedicati.
L'hardware riservato è conservato in locali chiusi a chiave e è accessibile solo ai dipendenti autorizzati.

## 3.1 Sicurezza delle apparecchiature

I server contenenti informazioni aziendali sono tenuti in un ambiente sicuro, protetto da:

1. Sicurezza fisica e controllo degli accessi
2. Dispositivi di spegnimento di incendi
3. Controllo della temperatura e dell'umidità
4. Basso rischio di infiltrazioni d'acqua
5. Alimentazione elettrica condizionata stabile protetta da gruppo di continuità e generatore stand-by, se possibile

Le apparecchiature di comunicazione chiave saranno anche protette da gruppo di continuità.
Le informazioni elettroniche sono mantenute sui server approvati dall'incaricato IT. 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 dall'incaricato IT o con il permesso dell'incaricato IT.
Fumare, bere e mangiare non è permesso nelle aree che ospitano apparecchiature informatiche.

## 3.2 Apparecchiature informatiche portatili e palmari

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. E' opportuno, pertanto, 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 dell'Organizzazione. L'apparecchiatura deve essere utilizzata solo dal personale a cui è stata rilasciata.
Tutte le dichiarazioni della politica riguardanti l'uso di software e giochi sono valide allo stesso modo per gli utenti di apparecchiature portatili appartenenti all'Organizzazione.
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.

### 3.3 Supporti rimovibili

I supporti removibili 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.

### 3.4 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. Una copia aggiuntiva deve essere conservata in un luogo distinto e sicuro, anche se il sistema di computer e tutte le altre copie vengono distrutte.
La distribuzione della documentazione di sistema deve essere autorizzata formalmente dal gestore.

## 4 Protezione di software e informazioni

### 4.1 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 Abaco 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. Abaco 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.

### 4.2 Software non autorizzato

Abaco consente che solo il software autorizzato venga installato sui propri PC. Abaco 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 assistenza IT. I pacchetti software devono rispettare e non compromettere gli standard di sicurezza Abaco. I giochi per computer non devono essere installati su workstation Abaco.

### 4.3 Controllo di virus

Abaco 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 assistenza IT per suggerimenti su antivirus.

### 4.4 Accesso alle informazioni

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 cancellare lo 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 terminali o PC 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.
Abaco 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 dell'Organizzazione devono avere una firma standard in cui si afferma:
"Questa e-mail e gli eventuali file trasmessi con questa e-mail sono riservati e sono destinati esclusivamente per l'uso del singolo o dell'ente a cui sono indirizzati. Il loro contenuto non può essere modificato. Se l'utente non è il destinatario stabilito di questa comunicazione, è pregato di avvisare il mittente e di eliminare e distruggere tutte le copie immediatamente. L'uso diretto o indiretto, la diffusione, la distribuzione o la copia non autorizzati di questo messaggio ed eventuali allegati è severamente proibito.
Ai sensi del Regolamento UE 2016/679, si precisa che le informazioni contenute in questo messaggio e negli eventuali allegati sono riservate e per uso esclusivo del destinatario. Persone diverse dallo stesso non possono copiare o distribuire il messaggio a terzi. Chiunque riceva questo messaggio per errore, è pregato di distruggerlo e di informare immediatamente il mittente."

## 5 Gestione degli assets (hardware)

### 5.1 Archivio hardware

Presso l'Organizzazione viene gestito e costantemente mantenuto un inventario di tutti i computer e le apparecchiature. L'incaricato 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. L'incaricato IT manterrà una copia dell'inventario ed effettuerà periodicamente un riesame dell'hardware sotto la responsabilità del Responsabile Protezione Dati.
Le regole per l'utilizzo accettabile degli assets associate alle strutture di elaborazione delle informazioni sono contenute nel documento "Istruzioni ai soggetti autorizzati" e sottoscritte da ciascun operatore al momento dell'assunzione.

### 5.2 Libreria software

Un registro aggiornato di tutto il software con licenza è mantenuto per garantire che l'Organizzazione sia a conoscenza delle proprie risorse e che siano seguite le condizioni di licenza. Questo registro è mantenuto dall'incaricato IT. I Responsabili Trattamento Dati hanno la responsabilità di informare l'incaricato IT dell'acquisto di qualsiasi software. L'incaricato IT mantiene una copia dell'inventario ed effettuerà periodicamente un riesame del software installato sotto la responsabilità del Responsabile Protezione Dati.

## 6 Continuità

### 6.1 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.
L'incaricato IT 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 o come definito nel piano di emergenza documentato per il sistema. 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.

## 6.2 Ripristino

Le modalità di ripristino vengono applicate per i seguenti motivi:

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

L'Organizzazione è 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, L'Organizzazione ha adottato misure per limitarne l'impatto, stabilendo l'ubicazione principale e di backup dei sistemi centrali in due sedi distanti tra loro.

### 6.2.1 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.

### 6.2.2 Server di rete

La resilienza è integrata nei server, ove possibile. È incluso l'utilizzo di tecniche di mirroring RAID per consentire la ricostruzione rapida dei dati e l'utilizzo di funzioni duali come alimentatori per ridurre l'impatto di un guasto hardware.

## 6.3 Apparecchiature, supporti e smaltimento di dati

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 l'incaricato IT, che farà in modo che i dischi vengano cancellati secondo gli standard di sicurezza.

# 7 Politica desktop

## 7.1 Politica hardware per computer desktop

### 7.1.1 Scopo e ambito della politica

Questa politica specifica nei dettagli quali piattaforme hardware sono utilizzate come standard per i computer desktop dell'Organizzazione e il livello di supporto previsto dall'incaricato IT.
La politica identifica e definisce:

1. Le piattaforme hardware per computer desktop supportate centralmente
2. Il livello di supporto che sarà fornito dal reparto di assistenza IT
3. suggerimenti relativi all'hardware per i centri di sviluppo
4. Le eccezioni alla politica.

### 7.1.2 Monitoraggio e riesame delle politiche

Il reparto di assistenza IT è responsabile dell'attuazione di questa politica e del suo sviluppo futuro. Il reparto di assistenza IT effettuea una revisione importante delle piattaforme hardware ogni anno. Eventuali revisioni proposte della politica sono discusse con la gestione di Abaco.

### 7.1.3 La politica

#### 7.1.3.1 Piattaforma hardware e specifiche

L'incaricato IT pubblica una specifica di sistema definendo i requisiti minimi per i PC desktop e laptop/notebook di proprietà dell'Organizzazione e le eventuali eccezioni ammissibili.
Questa specifica è riesaminata almeno una volta l'anno dall'incaricato IT sotto il controllo del Responsabile Protezione Dati.
Tutti i computer desktop e laptop di proprietà acquistati dall'Organizzazione per l'uso da parte del personale devono rispettare la specifica.

#### 7.1.3.2 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 dell'Organizzazione<br>Funzionamento efficace del software desktop standard<br>Funzionamento efficace e corretto di tutto il software supportato nelle categorie Standard Office IT e Infrastructure Tools (vedere Politica software per computer desktop)Queste categorie di software includono il software IT per | Anni 1-3<br>dopo l'acquisto |

| | | |
|---|---|---|
| | ufficio di base e il software antivirus installati sui desktop di proprietà di Abaco. | |
| 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<br>dopo l'acquisto |

L'obiettivo dell'Organizzazione 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 aziendale senza problemi e funzionare in modo soddisfacente, va riconosciuto che ciò non può essere garantito e l'incaricato IT non offrirà un supporto significativo per risolvere i problemi relativi a tali apparecchiature.
La Direzione è consapevole del rischio e del costo maggiore che implica il supporto di PC più vecchi di 5 anni e pianificano programmi di sostituzione IT per tali apparecchiature.
Il supporto dell'incaricato IT o la fornitura di servizi per computer desktop di proprietà dell'Organizzazione diversi dalla piattaforma hardware per desktop standard non sono garantiti. Tuttavia, qualora l'incaricato IT venisse a conoscenza di poter fornire supporto nella risoluzione dei problemi con altre piattaforme hardware, condividerà questa informazione con il personale.
L'incaricato IT 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 assistenza IT dai fornitori approvati Per le altre periferiche di uso comune come scanner, fotocamere digitali e PDA, il reparto di assistenza IT 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 Abaco 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.

#### 7.1.3.3 Approvvigionamento e distribuzione

L'incaricato IT fornisce consulenza di acquisto per la piattaforma hardware desktop standard, inclusi specifiche minime e modelli standard di fornitori approvati e stampanti desktop consigliate.
L'incaricato IT 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 dell'Organizzazione e le normative locali.

## 7.2 Politica software per computer desktop

## 7.2.1 Scopo e ambito della politica

Questa politica illustra nei dettagli come i sistemi operativi e altro software presenti sui computer desktop Abaco vengono distribuiti e supportati dall'incaricato IT. 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:

1. I sistemi operativi supportati a livello centrale
2. Il software applicativo supportato a livello centrale
3. Le eccezioni alla politica.

### 7.2.2 Monitoraggio e riesame delle politiche

L'incaricato IT è 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.

### 7.2.3 La politica

#### 7.2.3.1 Sistemi operativi supportati

Un sistema operativo desktop standard viene utilizzato per i computer desktop per i quali l'incaricato IT garantisce il supporto. I sistemi operativi supportati e le eventuali eccezioni sono elencati nell'appendice A - sistemi operativi supportati

### 7.2.4 Software applicativo supportato

L'incaricato IT fornisce il supporto completo per il software applicativo riportato nella appendice B. Questo software è disponibile per gli utenti anche attraverso l'installazione in rete (programmi annunciati). Il software non incluso nell'elenco può essere installato, ma non sarà supportato dal reparto di assistenza IT.

## 7.3 Approvvigionamento di computer desktop e politica di distribuzione

### 7.3.1 Scopo e ambito della politica

Questa politica illustra nei dettagli l'approvvigionamento e la distribuzione dei sistemi di computer desktop dell'Organizzaizone 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 con le strategie di approvvigionamento IT.
La politica identifica e definisce:

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

### 7.3.2 La politica

#### 7.3.2.1 Fornitori

L'ufficio Acquisti Centralizzati è responsabile di individuare i fornitori approvati per computer desktop, portatili e stampanti. Non ci saranno più di due fornitori per ciascuna delle seguenti categorie: computer desktop, portatili e stampanti. In alcuni casi potrà esserci un unico fornitore.
L'ufficio Acquisti Centralizzati (UAC) controlla le prestazioni del fornitore su una base costante.
Se le sue prestazioni sono state inaccettabili, il fornitore ne viene informato e UAC 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, UAC deciderà se e quando sostituire il fornitore. Un'analisi approfondita dei fornitori è eseguita da UAC in collaborazione con l'incaricato IT, 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.
UAC garantisce che qualsiasi disposizione di acquisto dell'Organizzazione con i fornitori di computer desktop e portatili sia in conformità con la legislazione nazionale ed europea emergente.

#### 7.3.2.2 Specifiche minime consigliate e modelli standard

L'incaricato IT riesamina e pubblica le specifiche minime consigliate e i modelli standard per computer desktop, portatili e stampanti. Le unità che acquistano sono tenuti a rispettare le specifiche minime consigliate.

#### 7.3.2.3 Distribuzione e smaltimento

Tutti gli uffici dell'Organizzazione devono avere una strategia di sostituzione continua per le apparecchiature IT (inclusi computer desktop e portatili) e attuare questa strategia nella procedura di compilazione del bilancio.
Questa strategia deve essere approvata dalla Direzione Generale con l'obiettivo di sostituire l'hardware secondo un ciclo quinquennale, con adeguata migrazione di apparecchiature al fine di raggiungere questo obiettivo. I piani di sostituzione degli uffici per i computer desktop e portatili dovrebbero essere coerenti con questo obiettivo.
Dopo cinque anni di funzionamento, 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 elettroniche.
Le apparecchiature possono anche essere donate a terzi, associazioni o singoli, purché la memoria sia completamente cancellata con procedure che impediscano il successivo recupero di dati.
Lo smaltimento o la donazione sono registrate nel registro degli asset.

# 8 Politica per la posta elettronica

## 8.1 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.
Attivando questa funzionalità, ogni volta che l'utente accede alla mail aziendale, oltre ad inserire nome utente e password, verrà inviato un codice tramite SMS al numero di telefono impostato, evitando in questo modo al malintenzionato di eseguire l'accesso. É possibile bypassare questa opzione inserendo il dispositivo client tra quelli autorizzati.

## 8.2 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 dell'Organizzazione 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 e- mail 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.

## 8.3 Virus e allegati

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

## 8.4 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.

## 8.5 Applicazione e controllo

Abaco si riserva il diritto di effettuare attività di controllo sui propri sistemi, anche senza preavviso. Abaco 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.

### 8.6 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.

## 8.7 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.

## 8.8 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.

## 8.9 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.

## 8.10 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.

# 9 Linee guida sugli antivirus

## 9.1 Cos'è un virus?

### 9.1.1 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.

### 9.1.2 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".

## 9.2 Azioni per prevenire la diffusione di virus e malware

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.

## 9.3 Prevenzione antivirus e malware implementata

Si è deciso di installare su ogni PC o assets assegnato ai dipendenti un antivirus e malware con licenza (AVG). La licenza del SW in questione ha validità 2 anni. All'interno di questi due anni l'antivirus si aggiorna automaticamente. Allo scadere della licenza, questa viene rinnovata e l'amministratore di sistema provvede all'aggiornamento su tutte le macchine.

## 9.4 Evitare il software non autorizzato

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.

## 9.5 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:

1. 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

2. Se è presente un messaggio ma sembra non avere senso
3. Se è presente un messaggio, ma sembra insolito da parte del mittente (sia nel contenuto che nel modo in cui è espresso)
4. Se riguarda materiale insolito
5. 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!")
6. 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 ...)
7. 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.

### 9.5.1 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.

### 9.5.2 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.

### 9.5.3 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.

**Appendice A – sistemi operativi supportati**

Il sistema operativo desktop standard alla data di aggiornamento del presente documento è è Microsoft Windows 7 a 64 bit.

Fanno eccezione:

- Sistemi di computer desktop diversi dai computer basati su processori Intel x86 compatibili (PC), 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 assistenza IT, 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 assistenza IT. 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. Nessun supporto viene garantito per altri sistemi operativi desktop diversi dal sistema operativo desktop standard, il relativo predecessore (vedere anche 3) e Linux (vedere 4), ma laddove il reparto di assistenza IT abbia consapevolezza di informazioni che potrebbero aiutare a risolvere un problema, tali informazioni saranno condivise. Il reparto di assistenza IT fornisce un servizio centrale per assicurare che il sistema operativo desktop standard possa essere corretto/aggiornato automaticamente su tutti i sistemi di proprietà di Abaco 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 assistenza IT aggiornare i server su base mensile. Il reparto di assistenza IT fornisce a ciascun reparto la possibilità di installare nuove workstation da immagini software, se possibile. È 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.

## Appendice B – software applicativi supportati

| Tipo | Software |
|---|---|
| Ufficio | Microsoft Office Word, Microsoft Office Excel, Microsoft Office Powerpoint, Microsoft Office Visio, OpenOffice, LibreOffice |
| E-mail | Microsoft Office Outlook<br>Mozilla Thunderbird Windows Mail |
| Antivirus | AVG |
| PDF | Adobe Acrobat Reader |
| VoIP | Skype |
| Messaggistica istantanea | Skype |
| Browser | Microsoft Internet Explorer, Mozilla, Firefox, Chrome |
| Virtualizzazione | VMware |
| Sviluppo (Java) | JDK Eclipse |
| Sviluppo (.NET) | Microsoft Visual Studio |
| Gestione progetti | Microsoft Office Project Project Control Center (PCC) CVS, SVN |