6.2.1 Politica per i dispositivi portatili

L'organizzazione, nell'ambito della propria **sede e al di fuori dei luoghi di lavoro**, ha stabilito che, per l'espletamento delle attività aziendali, quando opportuno, si impiegano i seguenti dispositivi di proprietà dell'organizzazione e concessi in uso al personale:

- Smartphone
- Tablet
- PC portatili

REGOLE DI IMPIEGO

L'impiego di tali dispositivi è disciplinato dalla eseguenti regole:

- Il dispositivo è ad uso personale
- Non può essere utilizzato da nessuno al di fuori dell'assegnatario
- Deve essere utilizzato solo ai fini lavorativi, non è previsto il byod (**bring your own device**, *uso promiscuo*)
- La manutenzione fisica del dispositivo è affidata all'assegnatario (ancorché supervisionata dall'asset manager)
- La protezione fisica del dispositivo è affidata all'assegnatario (ancorché supervisionata dall'asset manager)
- È vietato installare software, trattare file o gli altri programmi di utilità sul dispositivo ad eccezione di quelli predisposti dall'organizzazione o dal suo funzionamento
- È vietato collegare hard disk, chiavette USB e altri dispositivi di memoria al dispositivo

CONFIGURAZIONI PER LA SICUREZZA

Relativamente alle configurazioni, tutti i dispositivi impiegati all'esterno sono controllati da remoto. È la stessa organizzazione che provvede, tramite l'amministratore di sistema, e in maniera centralizzata, a:

- Impostare il controllo di accesso al dispositivo tramite autenticazione
- Installare, configurare, aggiornare e controllare l'antivirus
- Installare, configurare, aggiornare e controllare il firewall del singolo dispositivo
- Installare, configurare, aggiornare e controllare il software e i programmi di utilità

6.2.2 Telelavoro

Previsione contrattuali del telelavoro

La nostra organizzazione prevede che alcune attività lavorative possano essere eseguite all'esterno dei locali delle sue sedi ed in particolare in un ambiente idoneo a:

- Eseguire la prestazione lavorativa in maniera efficace ed efficiente almeno tanto quanto sarebbe "in ufficio"
- Custodire i necessari dispositivi di lavoro in maniera sicura
- Preservare la sicurezza delle informazioni contenute negli asset
- Consentire al lavoratore di poter godere del comfort "adeguato" e della necessaria concentrazione (assenza di distrazioni)

Il telelavoro è disciplinato, ai sensi di legge e conformemente alle specifiche normative in merito, dal contratto di lavoro che lega l'organizzazione al lavoratore, sia tale contratto di natura individuale o collettiva.

Responsabilità nel telelavoro

L'RDP (Produzione) ha la responsabilità:

- Della supervisione delle attività lavorative compiute in regime di telelavoro
- Della sicurezza delle informazioni ad esse associate
- Della predisposizione dei controlli di sicurezza

Telelavoro come misura per la business continuity

L'organizzazione considera il Telelavoro uno strumento efficace da impiegare quando condizioni improvvise ed avverse dovessero rendere impossibile il proseguire delle attività lavorative all'interno dei locali dell'organizzazione. Il telelavoro rappresenta, di conseguenza, anche una misura per la "business continuity".

Regole di prevenzione per il telelavoro

L'organizzazione, allo scopo di tenere sotto controllo i rischi per la sicurezza delle informazioni nell'ambito del telelavoro applica la politica di prevenzione basata sulle seguenti regole:

- Rende consapevole il personale, attraverso interventi di formazione, dei pericoli che possono compromettere la riservatezza, l'integrità e la disponibilità delle informazioni e dei controlli di sicurezza da applicare
- Fornisce i dispositivi portatili e vieta l'impiego di dispositivi personali
- Amministra il telelavoro con strumenti che permettono la pianificazione e la verifica delle attività eseguite da remoto
- Rende disponibile l'assistenza da parte dell'amministratore di sistema per la soluzione di problemi tecnici
- Rende disponibile l'assistenza da parte del RGSI per l'applicazione delle procedure di sicurezza
- Predispone apposite utility software per la rendicontazione del lavoro svolto da remoto
- Vieta l'impiego di "postazioni di lavoro" occasionali

9.1.1 Politica di controllo degli accessi

L'organizzazione, per proteggere la riservatezza delle informazioni, ha stabilito che solamente determinate persone possono accedere nei luoghi in cui esse sono custodite e trattate, siano essi luoghi di tipo fisico (aree riservate, cassaforte, archivi, etc.) oppure di tipo logico (hard disk, database, etc.).

COS'È IL CONTROLLO DI ACCESSO

Gli accessi alle aree di lavoro dell'organizzazione e gli accessi alla rete e ai servizi di rete sono controllati affinché soltanto coloro che sono stati espressamente autorizzati dall'alta direzione (e controllati dall'amministratore di sistema) possono accedere alle informazioni critiche trattate nei processi o comunque detenute a qualunque titolo (legittimo) dall'organizzazione stessa.

I REQUISITI DI BUSINESS DEL CONTROLLO D'ACCESSO

Il personale che lavora nei processi primari (operativi) deve accedere alle sole aree fisiche nelle quali si trattano informazioni relative ai processi primari e può accedere, tramite la rete dei computer, solamente a quelle aree di rete (cartelle/directory) che contengono informazioni relative ai processi primari.

Il personale impiegato nei processi di supporto deve accedere alle sole aree fisiche nelle quali si eseguono attività di supporto e si trattano informazioni appartenenti a tale categoria di processi.

Il personale impiegato nei processi di sicurezza delle informazioni invece è dotato di una maggiore libertà poiché, in ragione delle sue mansioni, deve poter intervenire sia fisicamente che telematicamente presso aree in cui si trattano le informazioni a prescindere dai processi a cui esse appartengono.

L'organizzazione ha stabilito che soltanto coloro che sono stati espressamente autorizzati possono accedere alle informazioni critiche trattate nei processi o comunque detenute a qualunque titolo (legittimo) dall'organizzazione stessa.

L'APPPLICAZIONE DEL CONTROLLO D'ACCESSO NELL'ORGANIZZAZIONE

Per questa necessaria limitazione, prevista dalla politica del controllo degli accessi con la finalità di proteggere le informazioni, l'organizzazione ha provveduto a individuare dei "controlli di accesso" previsti per:

- L'accesso alla sede aziendale
- L'accesso ai singoli uffici (aree riservate)
- L'accesso ai dispositivi da impiegare per gestire le informazioni (computer)
- L'accesso al sistema informativo aziendale
- L'accesso agli archivi cartacei
- L'accesso alla sala server (dove sono custoditi i server)
- L'accesso ai database che custodiscono informazioni di sicurezza (es. Database di password o di chiavi crittografiche)

9.4.3 Sistema di gestione delle password

Il sistema informativo dell'organizzazione permette di gestire dati e informazioni contenute all'interno del database del sistema informativo stesso. In questo database, **una tabella è riservata alla registrazione delle password** che, in ogni caso, rimangono **cifrate** e quindi non comprensibili.

La tabella delle password è stata predisposta per "accettare" le password che presentano le seguenti caratteristiche:

- Lunghezza minima della stringa di 8 caratteri
- Presenza di lettere minuscole (a-z)
- Presenza di lettere maiuscole (A-Z)
- Presenza di numeri arabi (0-9)
- Caratteri non alfanumerici (ad esempio: ?, #, *)

Il sistema prevede la scadenza della password decorsa la quale le password originarie non sono più attive e vanno sostituite con altre che rispettano i medesimi requisiti.

Il sistema fornisce all'utente un feedback in merito alla "sicurezza" della password scelta.

Più la password è complessa maggiore risulterà la sua efficacia protettiva in caso di attacco "brute force". Tale attacco infatti prevede che un software malevolo formuli **tante combinazioni di lettere e numeri** fin quando non individua quella giusta per accedere.

Di qui si comprende anche perché sono stati limitati a 4 i possibili tentativi di accesso. Poi il sistema si blocca.

Il sistema di gestione delle password è affidato al software appositamente concepito per gestire il controllo degli accessi al sistema informativo.

Tale software garantisce:

- Archiviazione e gestione delle password
- Condivisione, gestione e fornitura agli utenti delle password
- Reimpostazione remota delle password
- Gestione di sessioni privilegiate, accesso remoto e accesso automatico
- Controllo, conformità e report

10.1.2 Gestione delle chiavi crittografiche

CRITTOGRAFIA PER LE COMUNICAZIONI TRAMITE MAIL E CHAT RISERVATA

Per assicurare la riservatezza delle **comunicazioni in mail** che gli utenti inviano e ricevono tra loro e con le parti interessate (fornitori, clienti, consulenti, etc.), tutte le mail che contengono informazioni critiche di livello A sono sottoposte al controllo della ***firma digitale*.** I messaggi e i documenti sono **cifrati e autenticati grazie all'impiego di tale "firma".**

Il mittente che comunica attraverso la mail dell'organizzazione, con l'applicazione della firma digitale, appone "un'etichetta" al messaggio assicurando che esso sia stato prodotto da una persona ben precisa. La firma digitale inoltre permette all'organizzazione di garantire che il messaggio non possa essere modificato durante il suo percorso in rete.

La firma digitale, quale controllo applicato dall'organizzazione, come abbiamo già anticipato, è in grado di garantire:

- L'identità del mittente, fornendo la certezza su chi ha inviato **(autenticazione)**
- L'impossibilità, per il mittente, di negare di aver spedito tale messaggio **(non repudiation)**
- Che il messaggio sia ricevuto esattamente come è stato inviato **(integrità)**

IL MECCANISMO DI SICUREZZA ALLA BASE DELLA CRITTOGRAFICA ASIMMETRICA

L'organizzazione, come già dichiarato, impiega la **crittografia asimmetrica**. Tale tipologia impiega una coppia di chiavi per cifrare e decifrare i dati. In pratica, la chiave utilizzata dal mittente per cifrare i dati (algoritmo che rende le informazioni incomprensibili) è differente dalla chiave utilizzata dal destinatario per decifrarli.

I contenuti che transitano nella rete per raggiungere il destinatario, durante il tragitto non possono essere intercettati e resi comprensibili a terzi poiché **la chiave di decifratura non viaggia unitamente al messaggio inviato** ma è in possesso del solo destinatario certo, autentico. L'organizzazione attraverso l'impiego della crittografia "asimmetrica" assicura la riservatezza delle informazioni e consente che il messaggio ricevuto dal destinatario non possa essere ripudiato.

10.1.2 Gestione delle chiavi crittografiche

La tabella che segue stabilisce la maniera con la quale provvedere alla **cifratura delle informazioni critiche** da parte dell'organizzazione.

POLICY DEI CONTROLLI CRITTOGRAFICI DEI FILE E DEI SUPPORTI	
ASSET DA SOTTOPORRE A CIFRATURA	L'alta direzione, in relazione al livello di criticità delle informazioni da proteggere dal rischio di perdita della riservatezza, stabilisce quali supporti e quali file debbano essere coperti dal controllo crittografico nel modulo **MOD-710-M- Inventario degli asset**. La cifratura dei file o dei supporti che li custodiscono viene eseguita dall'RGSI (con l'ausilio dell'amministratore di sistema) attraverso il software reso disponibile dall'organizzazione e indicato, anch'esso, nel modulo **MOD-710-M- Inventario degli asset.** **CIFRATURA DEGLI ASSET** Gli asset sottoposti a cifratura dall'organizzazione sono: ▪ Gli hard disk del server ▪ I dati riposti in back sul cloud ▪ I supporti nei quali sono presenti i dati di configurazione dei dispositivi della rete ▪ I dischi dei personal computer portatili ▪ I dischi dei personal computer fissi ▪ La memoria degli smartphone ▪ Le credenziali di autorizzazione per l'accesso fisico tramite porte ▪ I campi dei database ▪ I supporti nei quali sono presenti i dati di configurazione dei dispositivi di sicurezza ▪ I software che conservano i dati scansionati, tracciati e copiati per la sicurezza del sistema informativo e della rete ▪ I segnali audio della comunicazione telefonica in voip interna all'organizzazione

11.1.1 Perimetro di sicurezza fisica

L'organizzazione protegge le informazioni dai pericoli di natura fisica che possono derivare dall'esterno. A tale proposito, l'organizzazione ha definito un perimetro di sicurezza fisica, a protezione delle informazioni e degli asset con i quali queste sono gestite e che sono indicati nel modulo **MOD-710-M- Inventario degli asset**.

I controlli predisposti per la sicurezza delle informazioni, che costituiscono il "perimetro di sicurezza aziendale", sono stati distinti dall'organizzazione in due tipologie:

Controlli per la sicurezza fisica:
che presiedono l'accesso nell'organizzazione da parte del personale, dei fornitori e delle altre parti interessate. Nella sicurezza fisica sono contemplate quelle misure che tendono a controllare i rischi provenienti da persone mal intenzionate, persone i cui atti possono essere mirati:

- All'accesso abusivo alle informazioni
- Al loro asporto fisico (mediante l'asporto dei supporti)
- Alla loro distruzione

Controlli per la sicurezza ambientale:
che presiedono la protezione degli asset da minacce legate al clima, alla temperatura, agli eventi climatici. Tali minacce possono comportare la distruzione parziale o totale degli asset e delle informazioni contenute al loro interno.

La sicurezza delle informazioni che dipende dagli **aspetti fisici ed ambientali** può essere messa a rischio, ad esempio, dalle seguenti minacce:

- Incendio
- Esplosione
- Blackout
- Allagamento
- Surriscaldamento

E in tali minacce aggiungiamo anche quelle che, anche se dipendenti dalle persone e non dagli eventi fisici o climatici, mettono a repentaglio la "sicurezza fisica" degli asset, quali:

- Intrusione fisica di malintenzionati con asporto o distruzione di apparati e sistemi
- Atti dolosi compiuti da chiunque anche se non direttamente legati all'organizzazione (atti vandalici, proteste, insurrezioni, estorsioni, ritorsioni)

11.2.5 Trasferimento degli asset

Apparecchiature, informazioni o software non possono essere portati all'esterno della sede dell'organizzazione senza preventiva autorizzazione da parte dell'alta direzione. Come accade per i dispositivi di memoria (o supporti) le apparecchiature che escono dall'organizzazione per un trasferimento, oltre ad essere accompagnate dai documenti di trasporto DDT, devono prevedere:

- La compilazione del modulo **MOD-710-P Trasferimento asset**
- L'autorizzazione da parte dell'alta direzione
- L'applicazione dei controlli di autenticazione per l'accesso, cifratura e backup
- Il trasporto a mezzo di un vettore qualificato (iscritto nell'albo dei fornitori)
- La supervisione da parte dell'RGSI

È necessaria inoltre l'apposizione, sull'apparecchiatura in uscita dalla sede dell'organizzazione, di un **segno distintivo non rimovibile**, tale da renderlo inequivocabilmente identificabile ed appartenente all'organizzazione (es: un'etichetta nascosta che reca il numero di *id* del supporto e il logo dell'organizzazione).

In caso di trasferimento, l'RGSI deve verificare la necessità di effettuare eventuali registrazioni di **assegnazione del supporto ad un nuovo responsabile**, per esempio, un nuovo asset manager.

11.2.6 Sicurezza delle apparecchiature e degli asset all'esterno delle sedi

All'esterno delle sedi dell'organizzazione, ad eccezione delle attività eseguite in regime di telelavoro dalle persone autorizzate, non si eseguono altre attività di lavoro.

Ove l'organizzazione intendesse predisporre l'esecuzione dell'attività lavorativa presso sedi esterne (appartenenti magari a terzi o comunque sotto il controllo altrui) tali sedi esterne dovranno possedere i medesimi requisiti di sicurezza applicati per la sede disciplinata in tale documento.

È opportuno indicare in tale paragrafo che l'organizzazione dispone della possibilità di accedere ad una sede alternativa nelle ipotesi in cui un eventuale disastro dovesse rendere impossibile il proseguimento delle attività operative nella sede disastrata.
Tale ipotesi è disciplinata dalla procedura di sicurezza **PSI-17 – Gestione continuità operativa della sicurezza delle informazioni.**

12.5.1 Installazione del software sui sistemi di produzione

L'installazione, l'aggiornamento del software di produzione, delle applicazioni e delle librerie è effettuato soltanto dal responsabile del sistema informativo che è **formato ed addestrato e installa il software previa adeguata autorizzazione** dell'alta direzione.

Il sistema informativo e le applicazioni che include per la gestione delle informazioni sono *"prodotti"* all'interno dell'organizzazione dal team di sviluppo informatico che coincide con il personale dell'ufficio marketing e quello dell'ufficio progettazione. Il supervisore dello sviluppo e del funzionamento del sistema è il **responsabile del sistema informativo**.

I controlli previsti sono i seguenti:

CONTROLLO	APPLICAZIONE
Sui sistemi di produzione è presente solo codice eseguibile approvato e non codice di sviluppo o compilatori	Nella area produzione del sistema informativo è presente solamente codice eseguibile approvato dal RDP (produzione)
Le applicazioni e i sistemi operativi vengono installati solo dopo test estensivi e completati con successo	I test eseguiti prima della delivery (passaggi da progettazione a produzione) sono condotti dall'RDP (produzione) che autorizza il passaggio del codice applicativo.
I test includono verifiche di usabilità, di sicurezza, sugli effetti su altri sistemi e di facilità d'uso e sono effettuati su sistemi separati (vedere controllo 12.1.4)	Il codice di sviluppo e l'impiego di compilatori è logicamente separato da quello della produzione ed è eseguito su dati presenti sul disco "progettazione" e non sul disco "produzione". RDP (produzione) provvede ai test di: ▪ Usabilità ▪ Sicurezza ▪ Facilità d'uso e in caso di esito positivo autorizza il trasferimento del codice dal disco progettazione al disco produzione.
È assicurato che tutte le corrispondenti librerie di programmazione vengano aggiornate	Le librerie delle applicazioni del sistema informativo sono aggiornate dal responsabile del sistema informativo e dall'RDP (produzione) in relazione alle esigenze di ricorrere a codice già sviluppato e testato da parte degli sviluppatori. Tali aspetti, dal punto di vista della sicurezza delle informazioni, sono tenuti sotto monitoraggio grazie al modulo: **MOD-710-G- Valutazione software**

12.6.1 Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche del sistema informativo che emergono durante il suo utilizzo da parte degli utenti devono essere:

- Rilevate
- Descritte
- Analizzate nelle loro cause
- Gestite con delle azioni

Il processo relativo alla gestione delle vulnerabilità tecniche del sistema informativo è governato dal **responsabile del sistema informativo**.

L'individuazione può avvenire grazie alla documentazione della vulnerabilità all'interno del modulo **MOD-710-G-Valutazione software,** e in questo caso l'RGSI provvederà a riportarle al responsabile del sistema informativo.

In caso di emergenza la vulnerabilità è comunicata e formalizzata con i mezzi più veloci a disposizione dell'organizzazione quali: sms, telefonate, mail. Tale comunicazione dovrà considerare il rischio di diffondere, involontariamente, le informazioni in merito alla presenza di una vulnerabilità tecnica anche al cospetto di mal intenzionati, perciò va effettuata in maniera assolutamente ***tempestiva e riservata***.

Se la vulnerabilità tecnica risultasse ascrivibile ad una "*non conformità*" in relazione a quanto predisposto dalla procedura **PROC-1010 - Non conformità e azioni correttive,** il responsabile del sistema informativo procederà a descrivere la non conformità rilevata permettendo di comprenderne la natura e/o la classe di appartenenza. Successivamente provvederà ad analizzare le cause della vulnerabilità tecnica e provvederà a gestirla attivando gli RDP oppure il personale necessario.

Tali attività condotte dal responsabile del sistema informativo sono documentate all'interno del modulo: **MOD-1010-A- Rapporto di non conformità**, in quanto l'organizzazione può riconoscere a tali vulnerabilità un "difetto di conformità" rispetto all'obiettivo strategico della sicurezza globale.

12.6.2 Limitazioni all'installazione del software

L'installazione di software estraneo all'organizzazione non è permessa a nessuno se non autorizzato dall'alta direzione e sotto il controllo dell'amministratore di sistema e del RGSI.

Tali installazioni, eventualmente concesse a servizio di prove e test, sono consentite su computer e reti assolutamente separati dalla rete.

13.1.1 Controlli di rete

La rete informatica dell'organizzazione è costituita dal server, che è il computer che fornisce i servizi alla rete, i personal computer sui quali gli autorizzati utilizzano il sistema operativo e le sue applicazioni. Poi ci sono tutti i dispositivi che permettono il funzionamento della rete nei collegamenti, nella trasmissione dei pacchetti di informazioni, nello smistamento e nella distribuzione dei servizi resi disponibili dall'alta direzione e documentati all'interno del modulo **MOD-710-M- Inventario degli asset**

La struttura della rete informatica dell'organizzazione è costituita da "asset" (server, computer, dispositivi). Tali sono stati **raggruppati in classi**, e ciascuno di esso è sottoposto a controlli di sicurezza atti a scongiurare i rischi relativi alla perdita della riservatezza, dell'integrità e della disponibilità delle informazioni.

Gli asset dell'organizzazione appartenenti alla classe **"Rete e comunicazioni"** sono impiegati tanto nei processi primari che trattano informazioni critiche di livello A e quanto nei processi secondari le cui informazioni trattate sono di livello B.

Tali asset sono i seguenti e funzionano nella maniera indicata:

- PROVIDER (Apparato di fornitura servizi Internet)
- CLOUD (Server remoto in cui le informazioni vengono duplicate e custodite)
- LAN (Rete locale interna all'organizzazione)
- SERVER POSTA ELETTRONICA (Computer che fornisce i servizi di posta elettronica all'organizzazione)
- SERVER CENTRALE (Computer che fornisce i servizi di rete all'organizzazione)
- ROUTER (Dispositivo che permette di interfacciare sotto-reti che sono: Primaria, Supporto e Sicurezza)
- SWITCH (Dispositivo di collegamento di altri dispositivi alla rete LAN)
- ACCESS POINT (Dispositivo per l'accesso wireless alla rete)
- CLIENT (Computer interni all'organizzazione collegati alla rete)
- CABLAGGIO (Cavi Ethernet e fibra ottica)
- TELEFONO

COSA PROTEGGERE

La sicurezza di ciascun asset, come documentato nell'inventario sopra indicato, è attribuita ad un **asset manager** che **presiede e verifica l'attuazione dei controlli** di sicurezza elencati dell'Annex A della Norma ISO 27001:2017 relativi a:

I dispositivi di elaborazione

Nei dispositivi di elaborazione, tenendo a parte il server e i servizi di cloud computing, l'organizzazione ha incluso:

- Computer
- Smartphone (considerati come sopra)

13.2.1 Politiche e procedure per il trasferimento delle informazioni

Trasferimento all'esterno di informazioni contenute nei file

I dati e le informazioni presenti all'interno del sistema informativo aziendale sono immessi ed elaborati:

- Dalle persone autorizzate all'interno dell'organizzazione
- Dalle persone autorizzate presso i clienti, i fornitori e le altre parti interessate.

Il sistema informativo, per quel che riguarda i processi primari, dispone del **software di produzione** specifico che permette di analizzare, classificare, gestire e trasformare le informazioni in un ambiente di lavoro condiviso nel quale, gli utenti eseguono le attività finalizzate all'ottenimento di un output ben preciso.

L'output può consistere in:

- Un **progetto interno** (funzionale ai processi interni dell'organizzazione)
- Un **progetto per un cliente** (il vero e proprio servizio che l'organizzazione rilascia al cliente che lo ha commissionato)

Questi output non sono solamente delle informazioni presenti sotto forma di ***record*** all'interno del database del sistema informativo ma sono dei **veri e propri documenti** (file) nei quali soni indicate le procedure ed i calcoli relativi al progetto (interno o esterno che sia). **Questi file "critici" sono l'oggetto fondamentale dei trasferimenti.**

Data la particolare criticità dei progetti (documenti), l'organizzazione ha provveduto a stabilire l'impiego di un **software di trasferimento file** che prevede un sistema di **autenticazione da parte del mittente e da parte del ricevente**.

Il trasferimento dei file avviene nella seguente maniera:

- Gli utenti autorizzati al trasferimento dei file **effettuano l'autenticazione** presso il software di trasferimento dei file
- **Caricano i file** da trasmettere in una (es: documenti per il cliente) "safe box" (memoria virtuale)
- Il software provvede alla **cifratura dei file**
- Il ricevente (es: personale del cliente o del fornitore) effettua **l'autenticazione** presso il software di trasferimento dei file
- Il software, a seguito dell'autenticazione del ricevente, **decifra i file** e li rende disponibili per il download
- Il **software traccia tutte le operazioni** e il suo impiego è monitorato dal software deputato al controllo dei log

Il software traccia le operazioni condotte nell'ambito delle attività del trasferimento: mittente, destinatario, durata di sessione, orari, file trasferiti, etc.

La sicurezza delle informazioni inerente al loro trasferimento (verso l'esterno e verso l'interno) è assicurata grazie alla gestione supervisionata di tali attività.

14.1.1 Analisi e specifiche dei requisiti per la sicurezza delle informazioni

Le informazioni che l'organizzazione intende proteggere sono gestite dal sistema informativo aziendale che possiamo identificare nella piattaforma software grazie alla quale l'organizzazione:

- Interagisce con i clienti somministrando il prodotto/servizio
- Interagisce con i fornitori per l'acquisizione di prodotti/servizi
- Esegue le attività produttive, attraverso i software connessi alla piattaforma
- Custodisce e rende disponibili i dati relativi ai processi

Il sistema informativo aziendale è costituito:

- Dal database che contiene tutte le informazioni
- Dalle pagine di accesso ai dati
- Dalle funzioni (oppure ulteriori software) che permettono di gestire ed elaborare i dati

I requisiti funzionali del sistema informativo

L'organizzazione, per eseguire le attività lavorative, ha determinato i requisiti funzionali che deve possedere il sistema informativo aziendale per rispondere alle esigenze informative ed operative dei ruoli che operano nei processi, nella maniera più efficace ed efficiente possibile. Essi sono ricostruiti attraverso la sequenza delle attività informatizzate che seguono le fasi dei processi.

Di seguito sono elencati i requisiti funzionali del sistema informativo.

REQUISITI RELATIVI AL CLIENTE *(COSA DEVE POTER ESEGUIRE IL CLIENTE GRAZIE AL SISTEMA INFORMATIVO)*
Il cliente, collegandosi attraverso Internet, al sistema operativo aziendale deve poter:
a) Effettuare la richiesta di servizio/prodotto e stabilirne i requisiti
b) Accedere alle condizioni contrattuali che disciplinano il servizio
c) Monitorare le attività produttive relative alle sue richieste
d) Fare richieste, porre quesiti, eccepire contestazioni, rilasciare autorizzazioni
e) Acquisire il prodotto/servizio
f) Usufruire dell'assistenza post vendita
g) Pagare il servizio
h) Consultare i responsabili dell'organizzazione

14.1.2 Sicurezza dei servizi applicativi su reti pubbliche

Il sistema informativo dell'organizzazione è un sistema **web based** al quale si accede attraverso Internet. Il personale che lavora da remoto, non presente in organizzazione, accede talora anche a delle applicazioni (programmi per lavorare) che sono distribuite attraverso la piattaforma del sistema operativo.

La sicurezza dei servizi applicativi **resi disponibili attraverso Internet** viene garantita dalle seguenti misure:

- Il **software applicativo è residente sul server** aziendale e non presente sui computer che accedono al sistema
- Di tale software, conformemente a quanto prevedono **i relativi contratti**, sono determinati: la proprietà intellettuale, le licenze di utilizzo, i canoni, gli interventi di modifica ed ulteriore sviluppo
- Il software **(codice sorgente)** è protetto dai dispositivi di sicurezza che sono stati predisposti per la protezione delle informazioni critiche quali: controllo di accesso, cifratura, backup, antivirus, etc.
- **Il software è documentato** e la sua documentazione, adeguatamente protetta alla stessa maniera del software, consente di comprenderne la struttura, le dinamiche, le funzioni e i servizi resi allo scopo di facilitare gli interventi di manutenzione.

L'organizzazione **non impiega reti pubbliche** intese quali quelle di solito messe a disposizione di utenti, clienti e visitatori di alberghi, ristoranti, stazioni ferroviarie, treni, impianti sportivi, centri turistici, etc.

14.1.3 Sicurezza delle transazioni nei servizi applicativi

LE COMUNICAZIONI IN RETE ATTRAVERSO IL SISTEMA INFORMATIVO

L'organizzazione gestisce le informazioni grazie all'impiego del suo sistema informativo. Tale sistema, come più precisamente illustrato nella procedura dedicata alla sicurezza del suo funzionamento, consente di trattare le informazioni attraverso le pagine web.

Le pagine web costituiscono le interfacce grazie alle quali l'utente può leggere, inserire e modificare le informazioni: per raccogliere i requisiti del cliente, per scrivere un progetto e per produrre i servizi, gli utenti autorizzati interagiscono con le pagine web.

Le pagine web del sistema informativo aziendale rendono visibili le informazioni presenti sul database del sistema informativo. Il protocollo impiegato per la comunicazione attraverso le pagine web è l'**HTTPS** (Hyper Text Transfer Protocol Secure). Grazie a questo protocollo che impiega la crittografia, le informazioni che i dipendenti, i collaboratori o gli utenti inviano non possono essere intercettate da una terza parte non autorizzata.

14.2.3 Riesame tecnico delle applicazioni in seguito ai cambiamenti

Lo schema proposto nel paragrafo precedente infatti costituisce uno degli input del riesame di direzione grazie al quale i responsabili dei processi RDP e coloro che sono incaricati della sicurezza delle informazioni effettuano la valutazione di impatto (riesame tecnico) e formulano le misure di prevenzione da adottare.

A seguito della valutazione di impatto, le decisioni assunte in merito a strategie di prevenzione da adottare in corrispondenza dei cambiamenti, sono documentate nel modulo **MOD-930-B- Verbale del riesame di direzione.**

14.2.4 Limitazione ai cambiamenti dei pacchetti software

Il software da adottare per il funzionamento del sistema operativo si basa, fondamentalmente sulle seguenti tecnologie:

- Linguaggio di programmazione: PHP
- Database: MySQL

Con il linguaggio di programmazione sono realizzate le pagine web di accesso ai dati che permettono di elaborare le informazioni presenti nel database MySQL.

Le decisioni riguardanti i cambiamenti dei pacchetti software devono documentare, nel modulo **MOD-930-B- Verbale del riesame di direzione**:

- I motivi dell'assoluta necessità del cambiamento
- Gli svantaggi conseguenti al cambiamento
- Le misure per gestire gli svantaggi conseguenti al cambiamento

L'analisi a tale riguardo può essere condotta attraverso lo schema riportato nei paragrafi precedenti in occasione dell'illustrazione della valutazione di impatto.

Le limitazioni ai cambiamenti dei pacchetti software si applicano in generale anche a:

- Software di sistema: quello relativo al **sistema operativo** Windows
- Software di base: insieme dei programmi e delle procedure di utilità
- Software applicativo, per gli uffici, scelto dall'organizzazione che è **Microsoft Office**

16.1.1 Responsabilità e procedure

Introduzione al disaster recovery plan dell'organizzazione

A fronte dei rischi che incombono sulle informazioni, l'organizzazione ha già stabilito i controlli di sicurezza interni che mantengono il rischio generale ad un livello basso. Tali controlli sono documentati all'interno del **MOD-710-M- Inventario degli asset**. La probabilità tuttavia che determinati incidenti possano accadere, ancorché bassa, non rende impossibili tali eventi.

Se i controlli applicati *internamente alla struttura*, finalizzati alla protezione delle informazioni dovessero risultare, **in condizioni critiche, inefficaci, compromessi, o comunque non funzionanti,** l'organizzazione mette in atto delle azioni la cui finalità è quella di poter **riacquisire, nel più breve tempo possibile, la disponibilità delle informazioni.**

Scopo

La presente procedura ha lo scopo di disciplinare la modalità con cui l'organizzazione gestisce la sopravvenuta indisponibilità delle informazioni causata dalla distruzione dei supporti residenti nella sua struttura fisica (locali, uffici e sala server).

Le cause della distruzione dei supporti, come abbiamo visto nell'identificazione e la valutazione dei rischi, possono consistere in fenomeni fisici o atmosferici quali ad esempio:

- Allagamenti
- Terremoti
- Alluvioni
- Incendi

La presente procedura, che scaturisce dall'analisi e dalla valutazione dei rischi, rappresenta il **DISASTER RECOVERY PLAN** che, tradotto in italiano va inteso come il **Piano di recupero delle informazioni da attuare in caso di disastro**.

L'organizzazione, in generale, per il recupero delle informazioni non più disponibili, adotta il "**backup**" la cui politica ed il cui funzionamento sono disciplinati nella procedura di sicurezza **PSI-12 – Sicurezza operativa**, nel paragrafo dedicato.

L'organizzazione adotta una soluzione di **disaster recovery** (di cui il backup è solo una componente) che è stata progettata in relazione alle caratteristiche tecniche della struttura IT. Ovviamente **l'infrastruttura di backup** è stata realizzata compatibilmente con quelle che sono le **possibilità di finanziamento** dell'organizzazione.

Dal punto di vista tecnico, la **soluzione di disaster recovery** tiene conto della quantità di informazioni che potrebbe "andare persa" a causa di un evento disastroso. Questa quantità è proporzionale al tempo che intercorre dal momento di produzione di un dato (ad esempio la creazione di un file sul computer da parte di un utente) al momento in cui questo dato viene salvato anche sul disco del server e del cloud e viene messo in sicurezza grazie all'operazione di backup.

16.1.1 Responsabilità e procedure

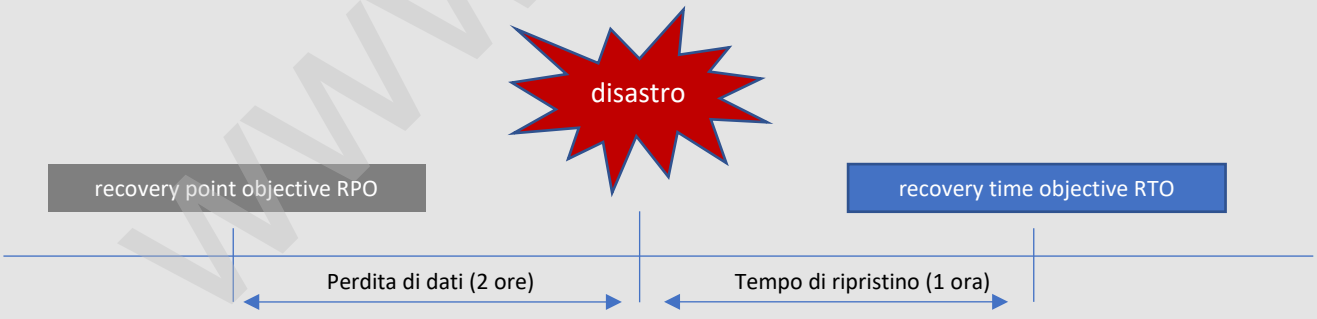
Per il "ricovero" delle informazioni, l'organizzazione ha optato per un'infrastruttura informatica **completamente ridondante con dati replicati fuori sede**. Attraverso il backup, infatti, le informazioni sono automaticamente copiate sul "**cloud**" del provider che, fisicamente, è distante più **di 75 km** dalla sede dell'organizzazione. Le best practices infatti, in materia di disaster recovery, suggeriscono un sito distate almeno 75 km allo scopo di dislocare le informazioni che potrebbero andar perse a causa di una calamità naturale (es: terremoto).

Di seguito l'organizzazione ha calcolato il tempo necessario per ripristinare le informazioni perse e riorganizzare le attività lavorative che si sono interrotte a causa di un incidente.

L'organizzazione ha stabilito l'RPO

Il Recovery Point Objective (RPO) rappresenta il massimo tempo che deve intercorrere tra la produzione di un dato e la sua messa in sicurezza (attraverso backup) e, di conseguenza, offre la misura della massima quantità di dati che il sistema informativo potrebbe perdere a causa di guasto improvviso. Tale RPO, nell'organizzazione, è di 2 ore.

Se si verifica il disastro, l'organizzazione dispone di tutte le informazioni (senza perderne alcuna) che vengono integralmente salvate ogni due ore.



L'organizzazione ha stabilito l'RTO

Il Recovery Time Objective (RTO) è il tempo di ripristino che occorre per il totale recupero dell'operatività dei processi. L'organizzazione ha stabilito l'RTO a 1 ora. Grazie al recupero delle informazioni perdute a causa del disastro si è teoricamente ***in grado di ripartire subito a meno che non sia stata compromessa le struttura dell'organizzazione.***

17.1.1 Pianificazione della continuità della sicurezza delle informazioni

Questa procedura, dal punto di vista logico e sequenziale, è connessa a quella che disciplina il disaster recovery plan e cioè la procedura di sicurezza **PSI-16 – Gestione degli incidenti relativi alla sicurezza delle informazioni.**

L'organizzazione, attraverso tale procedura infatti, persegue lo scopo di continuare ad operare (e produrre) in condizioni di crisi, assicurando, anche in queste circostanze eccezionali, la sicurezza delle informazioni dai rischi di perdita della riservatezza, dell'integrità e della disponibilità. I contenuti di questa procedura perciò approfondiscono con maggiore dettaglio le attività che l'organizzazione compie per "continuare a lavorare" a seguito dell'incidente che ha compromesso la sua "continuità operativa".

Con il **disaster recovery** che l'organizzazione ha documentato all'interno della procedura di sicurezza **PSI-16 – Gestione degli incidenti relativi alla sicurezza delle informazioni** (spesso confuso con la continuità della sicurezza delle informazioni), l'attenzione era focalizzata sul **recupero delle informazioni** e sulle azioni da compiere affinché queste ritornassero disponibili agli utenti del sistema operativo.

L'attenzione, in questo processo focalizzato sulla continuità operativa che è cosa diversa dal disaster recovery, si sposta sul ripristino delle attività basilari ***(processi produttivi verso il cliente)*** e sul funzionamento di queste, in condizioni di sicurezza per le informazioni, **nonostante le difficoltà dovute all'impossibilità temporanea di operare in condizioni ottimali.**

Al ***disaster recovery plan***, quello cioè documentato attraverso le azioni di ripristino della disponibilità dei dati, aggiungiamo il ***business continuity plan*** e cioè la pianificazione delle azioni che devono essere compiute **dalla rilevazione del "disastro" fino al ripristino e alla gestione dei processi basilari**, quelli cioè che, devono essere in funzione per non interrompere il rapporto con il mercato.

I processi critici per la continuità operativa

Se l'organizzazione, a seguito di un disastro, dovesse trovarsi nelle condizioni di dover continuare a produrre senza interruzioni (che potrebbero pregiudicare la continuità operativa del suo business), dovrebbe avere la possibilità di:

- **Attivare immediatamente il suo sistema informativo e le sue applicazioni**
- **Rendere le informazioni nuovamente disponibili in condizioni sicure.**

Tutto questo è possibile nell'ipotesi in cui, nonostante il disastro, il personale dell'organizzazione che lavora al sistema informativo possa rimanere alla propria postazione. Es: l'organizzazione sta subendo attacco informatico che compromette l'integrità delle informazioni presenti nel database del sistema informativo.

In questo caso l'organizzazione, avendo sottoscritto un contratto per il quale il proprio sistema informativo e i propri dati sono custoditi su un cloud di un provider, **provvede semplicemente a spostare l'attività operativa** degli utenti dal sistema informativo compromesso dal virus e residente sul server centrale interno, al sistema informativo "copia" residente sul cloud del provider.

17.1.3 Verifica, riesame e valutazione della continuità della sicurezza delle informazioni

L'organizzazione ha progettato la modalità con cui gestisce una situazione di crisi per assicurare la continuità operativa e la relativa sicurezza delle informazioni.

Una volta all'anno, la situazione di crisi, per quanto possibile, viene simulata allo scopo di verificare:

- La disponibilità immediata del sito alternativo
- La capacità di reperire le risorse necessarie al trasferimento e all'attivazione dell'altro sito
- I tempi di risposta del personale
- L'effettiva disponibilità delle informazioni
- Il funzionamento efficace dei processi di business in un contesto di emergenza

La simulazione, per condurre a dei risultati realistici, viene avviata dall'alta direzione in accordo con l'amministratore di sistema in maniera del tutto realistica. Il personale allertato e coinvolto, durante l'esercitazione, anche se consapevole che si tratta di una semplice simulazione, deve dare evidenza di essere pronto ad eseguire le funzioni di ripristino nei tempi concordati.

L'organizzazione, con tale simulazione dell'emergenza, effettua il riesame delle azioni pianificate valutando la sua capacità di fronteggiare in tempo, e in sicurezza, gli imprevisti dipendenti dai disastri.

Tale riesame è analogo a quello indicato nella procedura relativa al ricovero e al ripristino della disponibilità delle informazioni **PSI-16 – Gestione degli incidenti relativi alla sicurezza delle informazioni.**

Gli esiti della simulazione di un trasferimento nella sede di emergenza costituiscono oggetto di riesame della direzione solamente una volta all'anno. In quella occasione, devono essere documentati tra gli input di riesame di direzione in corrispondenza e in concomitanza degli input riguardanti **le evidenze relative agli incidenti della sicurezza**.

17.2.1 Disponibilità delle strutture per l'elaborazione delle informazioni

La ridondanza delle strutture per l'elaborazione dei dati è assicurata nella misura tale da permettere all'organizzazione di continuare ad operare in riferimento ai soli processi ritenuti critici e cioè quelli che, durante la crisi, mantengono in vita i rapporti con il cliente ed i fornitori.

La disponibilità di computer e dispositivi è, in parte, assicurata dalla loro presenza ridondante all'interno della stessa struttura operativa dell'organizzazione. Essa è assicurata inoltre dal contratto di servizio che l'organizzazione ha sottoscritto per usufruire del sito alternativo e delle risorse contenute al suo interno.

18.1.1 Identificazione della legislazione applicabile e dei requisiti contrattuali

La protezione delle informazioni, che è l'obiettivo strategico dell'organizzazione perseguito attraverso il presente sistema di gestione, deve essere progettata, concepita ed attuata in relazione ai requisiti della Norma ISO 27001 e i controlli da essa predisposti.

Questa conformità è spiegata, rispettivamente, all'interno delle procedure gestionali e all'interno delle procedure di sicurezza. Ci sono tuttavia altri requisiti che l'organizzazione deve rispettare nella sua attività di protezione delle informazioni che sono:

- **I requisiti contrattuali**
  Che l'organizzazione raccoglie e riesamina secondo quanto disciplinato dalla procedura **PROC-812- Requisiti.** Questi requisiti sono espressi **dal cliente** e riguardano il livello di sicurezza delle informazioni atteso dal cliente. Il cliente esprime i requisiti di *"sicurezza per le sue informazioni"* che dovranno essere elaborate dall'organizzazione in riferimento a precisi level service agreement (livelli di servizio). Tutto l'apparato di sicurezza dell'organizzazione è stato concepito per coprire le esigenze di sicurezza dei committenti.

- **I requisiti previsti dalla legislazione vigente**
  Che sono requisiti imposti da leggi che perseguono finalità che, in qualche modo, sono connesse o comunque possono essere influenzate dalla maniera in cui l'organizzazione protegge le informazioni. La legislazione in riferimento è la seguente:

  - Il Regolamento Europeo sulla protezione delle persone fisiche in riferimento ai dati personali n. 679/2016 (GDPR)
  - Il Provvedimento del Garante: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema n. 27 novembre 2008
  - L'Art. 2.8 della legge sul diritto d'autore (L. 633/41), in riferimento alla proprietà intellettuale del software

Il comportamento delle persone che elaborano le informazioni all'interno dell'organizzazione, oltre ad essere determinato dalle procedure che disciplinano i controlli di sicurezza è anche regolato dalla legge. Gli attentati alla sicurezza delle informazioni, oltre ad essere scongiurati dai controlli e dalle misure di prevenzione sono previsti e puniti anche dal codice penale.

L' articolo **615-ter del codice penale** prevede l'**accesso abusivo ad un sistema informatico** contro il consenso esplicito o implicito della persona avente diritto di escludere terzi dall'ottenimento di tale accesso. La pena è la reclusione fino a 3 anni.

18.1.2 Diritti di proprietà intellettuale

Considerazioni dell'organizzazione sui diritti di proprietà del software

L'ordinamento italiano, a seguito del recepimento delle norme europee quali la direttiva 2009/24/EC, ammette la tutela dei programmi per elaboratore tramite l'A**rt. 2 comma.8 della legge sul diritto d'autore (L. 633/41) aggiornata**, il quale stabilisce che sono ricompresi nella protezione "i programmi per elaboratore, in qualsiasi forma espressi purché **originali quale risultato di creazione intellettuale dell'autore**. Il termine "programma" comprende anche il materiale preparatorio per la progettazione del programma stesso.

Il copyright (diritto di copia) permette al suo titolare di controllare l'utilizzo finalizzato allo sfruttamento economico di un'opera dell'ingegno, in questo caso del programma per elaboratore. Tale possibilità discende dal riconoscimento dei diritti esclusivi di tipo patrimoniale del software, ex Art. 64-bis della legge sulla protezione del diritto d'autore, la cui normativa si configura come una **specificazione delle norme generali in materia di diritti economici** sanciti in generale per tutte le opere dell'ingegno dagli Artt. 12-19 della legge sulla protezione del diritto d'autore.

Scelte dell'organizzazione

L'organizzazione provvede a disciplinare gli eventuali oggetti del contendere, indicati nella tabella precedente, attraverso contratti che, conformemente a quanto prevede la legge sulla protezione del diritto di autore **L. 633/1941**, regolano la produzione di sistemi e di software che viene scambiato tra l'organizzazione e:

- I dipendenti (contratto di lavoro)
- I fornitori/consulenti (contratto di fornitura e accordi quadro)
- I clienti (contratto e specifiche di commessa)

L'organizzazione, ai fini di un'agevole risoluzione della controversia, ha stabilito che il software che gli eventuali contendenti vogliono rivendicare, deve essere depositato presso il **Registro Pubblico Speciale per Programmi per Elaboratore** oppure depositato come opera inedita qualora il software stesso non sia ancora stato pubblicato o utilizzato.

Ricorso al brevetto

Se l'organizzazione dovesse ritenere che il "proprio" software disponga degli speciali requisiti (creatività, originalità) previsti dalla normativa relativa alle "invenzioni", provvederà a brevettare il software controllando:

- Il diritto di sfruttamento economico del software
- Il diritto di effettuare o autorizzare:
  - La riproduzione, traduzione, adattamento, trasformazione, modificazione
  - La distribuzione in qualsiasi forma