CitNOW

CitNOW Politica sulla sicurezza informatica e dei dati

Ultimo aggiornamento:
Settembre 2017

Sistema/i di business CitNOW: Tutti i Riferimenti: ISO/IEC 27001 e 27002

Indice

Allegato

1. Politica sulla sicurezza dei dati

1.1 Panoramica generale

I dati costituiscono una risorsa essenziale per la nostra azienda. I dati che archiviamo comprendono: nomi di clienti, indirizzi e-mail, numeri di cellulare, targhe dei veicoli, informazioni eVHC dei clienti, dati di natura amministrativa, finanziaria e relativi al personale, rete di calcolo e sistemi di database, codice e script informatici. Qualsiasi sia la forma della loro raccolta, accesso o utilizzo, garantiremo la protezione dei dati tramite idonee misure di sicurezza, consentendoci di soddisfare i nostri obiettivi aziendali, conformemente alla normativa applicabile, e i nostri obblighi contrattuali.

1.2 Scopo

Il nostro obiettivo in termini di sicurezza è quello di proteggere la nostra azienda da problemi di sicurezza come: accesso non autorizzato ai sistemi, violazioni della riservatezza (persone che acquisiscono o diffondono informazioni in modo improprio), integrità (informazioni alterate o erroneamente convalidate, in modo volontario o accidentale) e disponibilità (informazioni non disponibili quando necessario) o qualsiasi altra questione che potrebbe incidere negativamente sulle nostre attività o sulle attività dei nostri clienti e fornitori.

1.3 Ambito

La presente politica riguarda tutti i sistemi informatici, i server e il software da noi gestito.

1.4 Politica

1.4.1 Approccio

C'impegniamo a:

Adottare ogni misura di sicurezza ragionevole, appropriata, pratica ed efficace per proteggere i nostri processi e le nostre risorse per raggiungere il nostro obiettivo di sicurezza.

Utilizzare un ISMS secondo la norma ISO/IEC 27001 come quadro di riferimento che ci guidi nel nostro approccio alla gestione della sicurezza.

Rivedere costantemente il nostro utilizzo delle misure di sicurezza affinché possiamo migliorare il modo in cui proteggiamo la nostra azienda.

Proteggere e gestire le nostre risorse informatiche per consentirci di rispondere alle nostre responsabilità contrattuali, legislative e di tutela della privacy.

1.4.2 Responsabilità

Tutti i dipendenti, passati e presenti, permanenti e temporanei, agiranno sempre in modo responsabile, professionale e sicuro avendo chiari i concetti alla base di questa Politica e impegnandosi a rispettarla.

Tutti i dipendenti rispetteranno le informazioni di proprietà di soggetti terzi, indipendentemente dal fatto che tale approccio sia richiesto o meno contrattualmente o legalmente.

Tutti i dipendenti aventi responsabilità di vigilanza sono tenuti a promuovere attivamente le migliori prassi tra il personale sul quale devono vigilare.

Il nostro CISO - che riporta direttamente al nostro CEO - è responsabile di garantire che i dati all'interno della nostra azienda siano adeguatamente protetti e che il nostro obiettivo di sicurezza venga raggiunto. Il CISO e il team incaricato della sicurezza sono autorizzati dal CEO a realizzare le attività e gli interventi necessari per contribuire al raggiungimento del nostro obiettivo di sicurezza, coerentemente con la presente Politica sulla sicurezza dei dati.

Il CISO potrà, di volta in volta, delegare alcune attività a singoli responsabili e ha l'incarico di allocare risorse sufficienti in modo da poter raggiungere il nostro obiettivo di sicurezza.

1.4.3 Prassi

Identificheremo i nostri rischi in materia di sicurezza e le relative priorità, rispondendo prontamente e attuando misure adeguate, efficaci e pratiche.

Tutti i dati (compresi quelli personali e di soggetti terzi) saranno protetti da controlli di sicurezza e da procedure di gestione appropriati al loro livello di sensibilità e criticità.

Qualora sia consentito, i dati saranno comunicati a soggetti terzi esterni alla nostra azienda. I titolari dei dati avranno la responsabilità di identificare a chi possono essere comunicati i propri dati e conserveranno registri completi e accurati di tali comunicazioni.

Garantiremo che le nostre attività possano continuare con interruzione o conseguenze minime qualora si verifichi qualsiasi tipo di problema o incidente di sicurezza.

Eventuali incidenti di sicurezza, reali o sospetti, saranno tempestivamente comunicati al team incaricato della sicurezza, il quale gestirà l'incidente e provvederà a un'analisi dei fatti per comprendere il problema. Gli incidenti di sicurezza correlati all'uso di dati personali saranno gestiti conformemente alla normativa sulla privacy applicabile.

Procedure e standard documentati, insieme a formazione e didattica, supporteranno questa Politica.

La conformità alla Politica sarà monitorata regolarmente dal team incaricato della sicurezza, che si incontrerà periodicamente.

Il nostro CISO realizzerà una revisione su base annua della Politica redatta dal team incaricato della sicurezza. Questa sarà oggetto di revisione per verificarne la completezza, l'efficacia e la fruibilità. L'efficacia sarà misurata in base alla nostra capacità di evitare incidenti di sicurezza e ridurre al minimo le eventuali conseguenze.

Il nostro CISO approverà tutte le nuove versioni della Politica sulla sicurezza dei dati. Tutti i nostri dipendenti hanno la responsabilità di identificare in che modo la Politica sulla sicurezza dei dati possa essere migliorata.

Eventuali suggerimenti di miglioramento devono essere inviati al team incaricato della sicurezza. Qualora si rendano necessarie modifiche immediate, verrà indetto un incontro speciale del team incaricato della sicurezza; altrimenti, i suggerimenti saranno discussi durante la riunione di revisione annuale della Politica.

1.4.4 Conoscenza della Politica

Una copia della presente Politica sarà resa disponibile a tutti i dipendenti attualmente impiegati o ai nuovi collaboratori che entrino in azienda. Le singole sezioni della Politica saranno aggiornate come necessario e saranno rese disponibili sul nostro Intranet Podio. Tutti i nostri dipendenti sono tenuti ad acquisire familiarità e ad attenersi sempre alla Politica sulla sicurezza dei dati. I membri del team incaricato della sicurezza saranno le prime persone responsabili di interpretare e chiarire il contenuto della Politica sulla sicurezza dei dati. I dipendenti che richiedano maggiori informazioni su uno o più aspetti della Politica dovranno discutere le proprie necessità con un membro del team incaricato della sicurezza.

1.4.5 Applicabilità e applicazione

La presente Politica si applica a tutti i nostri dipendenti e a coloro che utilizzano le infrastrutture e i dati della nostra azienda. La conformità alla Politica costituisce parte integrante del contratto di impiego e tutti i dipendenti saranno responsabili delle proprie azioni in materia di sicurezza dei dati.

Il mancato rispetto della Politica sulla sicurezza dei dati potrebbe ridurre la nostra capacità di raggiungere i nostri scopi e obiettivi di sicurezza e potrebbe danneggiare la reputazione professionale dell'azienda. La mancata conformità sarà, come misura estrema, gestita come questione disciplinare. Il nostro CISO sarà responsabile di tutte le decisioni relative all'applicazione di questa Politica e adotterà le procedure disciplinari a propria disposizione secondo le esigenze.

Promuoveremo l'adozione e l'utilizzo di questa Politica sulla sicurezza dei dati da parte di soggetti terzi che collaborano tramite joint venture..

2. Politica sulla sicurezza dei server

2.1 Panoramica generale

I server vulnerabili e non sicuri continuano a essere un importante punto di accesso per gli aggressori informatici. Politiche coerenti di installazione dei server, gestione della proprietà e della configurazione costituiscono una base di partenza importante.

2.2 Scopo

Lo scopo di questa Politica è definire degli standard per la configurazione di base delle attrezzature interne dei server, di proprietà e/o gestite dalla nostra azienda. Un'implementazione efficace di questa Politica ridurrà al minimo l'accesso non autorizzato alla nostra tecnologia e alle nostre informazioni proprietarie.

2.3 Ambito

Tutti i dipendenti, appaltatori, consulenti, collaboratori temporanei e altre figure presenti all'interno della nostra azienda e delle nostre affiliate devono attenersi alla presente Politica. Essa si applica ad apparecchiature quali i server da noi possedute, gestite, noleggiate o registrate sotto un dominio di rete interno di nostra proprietà.

2.4 Politica

2.4.1 Requisiti generali

Tutti i server impiegati dalla nostra azienda devono essere gestiti da un gruppo operativo, responsabile dell'amministrazione dei sistemi. Tutti i server che elaborano i dati dei clienti devono essere gestiti dal gruppo DevOps. Ogni gruppo operativo ha l'incarico di definire e mantenere delle linee guida approvate per la configurazione dei server sulla base delle necessità operative, dietro approvazione del team incaricato della sicurezza. I gruppi operativi devono monitorare la conformità della configurazione e attuare una politica di eccezione in base al proprio ambiente. Ogni gruppo operativo deve definire un processo di modifica delle linee guida per la configurazione, che comprenda revisione e approvazione da parte del team incaricato della sicurezza. È necessario soddisfare i seguenti criteri:

- Tutti i server devono essere registrati in DevOps. Come requisito minimo sono necessari i seguenti dati per identificare concretamente il punto di contatto:
- contatto/i e ubicazione dei server, e un contatto di riserva
- Hardware e sistema operativo/versione
- Principali funzioni e applicazioni, ove applicabile
- I dati comunicati a DevOps devono essere mantenuti aggiornati
- Le modifiche di configurazione per i server di produzione devono seguire le idonee procedure di gestione dei cambiamenti

A scopo di sicurezza, conformità e manutenzione, il personale autorizzato potrà monitorare e ispezionare attrezzature, sistemi, processi e traffico di rete.

2.4.2 Requisiti di configurazione

La configurazione del sistema operativo deve avvenire conformemente alle linee guida approvate del team incaricato della sicurezza.

Servizi e applicazioni non utilizzati devono essere disabilitati ove ciò risulti più pratico.

L'accesso ai servizi deve essere tracciato all'interno di un log e/o protetto da metodi di controllo degli accessi come un firewall web, se possibile.

Le patch di sicurezza più recenti devono essere installate sul sistema non appena possibile; l'unica eccezione è qualora l'immediata applicazione delle patch interferisca con i requisiti operativi.

I rapporti fiduciari tra sistemi costituiscono un rischio per la sicurezza e ne è sconsigliato l'utilizzo. Non usare un rapporto fiduciario quando un altro metodo di comunicazione risulta sufficiente.

Utilizzare sempre i principi di sicurezza standard dell'accesso di livello minore per eseguire una funzione. Non usare l'account root quando basta un account senza particolari privilegi.

Se è disponibile (ovvero tecnicamente possibile) un metodo per garantire una connessione su un canale sicuro, l'accesso privilegiato deve essere effettuato su canali sicuri (es. connessioni di rete codificate con SSH o IPSec).

I server devono essere fisicamente ubicati in un ambiente ad accesso controllato.

I server non possono in alcun caso essere ubicati all'interno delle nostre sedi/uffici.

2.4.3 Monitoraggio

Tutti gli eventi correlati alla sicurezza su sistemi critici o sensibili devono essere registrati in log e gli audit trail salvati come segue:

- Tutti i log correlati alla sicurezza saranno conservati online sul server per almeno 1 settimana.
- Il log deve essere configurato in modo da essere trasferito al server globale dei log per la sua archiviazione e conservazione.

Gli eventi correlati alla sicurezza saranno comunicati al team incaricato della sicurezza, il quale analizzerà i log e gli eventi. Verranno poi attuate le misure correttive necessarie. Gli eventi correlati alla sicurezza comprendono, in via non limitativa:

- Attacchi Port-Scan
- Prova di accesso non autorizzato ad account privilegiati
- Eventi anomali non collegati ad applicazioni specifiche sull'host

2.5 Conformità alla Politica

2.5.1 Misurazione dalla conformità

Il team incaricato della sicurezza verificherà la conformità alla presente Politica attraverso vari metodi, compresi in via non limitativa: ispezioni fisiche periodiche, report degli strumenti di business, audit interni ed esterni e feedback da parte del titolare della Politica.

2.5.2 Eccezioni

Eventuali eccezioni alla Politica dovranno essere precedentemente approvate dal team incaricato della sicurezza.

2.5.3 Non conformità

Qualora un dipendente violi la presente Politica, potrà essere sottoposto ad azione disciplinare, che potrebbe culminare nella risoluzione del rapporto di lavoro.

3. Politica di controllo e smaltimento delle risorse it

3.1 Panoramica generale

Tutto il personale e i dipendenti che hanno accesso ai sistemi informatici dell'azienda devono attenersi alla politica di controllo delle risorse IT definita di seguito per proteggere la sicurezza della rete, l'integrità dei dati, nonché proteggere e controllare i sistemi informatici e le risorse aziendali. La politica di controllo delle risorse non solo consentirà di tracciare le risorse aziendali per conoscere la loro ubicazione e chi le sta utilizzando, ma proteggerà anche tutti i dati in esse conservati. Questa politica sulle risorse riguarda anche il loro smaltimento.

Le risorse IT non vanno confuse né tracciate con altre risorse aziendali come gli arredi. Oltre al controllo e al tracciamento del patrimonio, uno dei principali motivi per tracciare le risorse IT è la sicurezza informatica. Una specifica politica di tracciamento delle risorse IT consentirà all'azienda di adottare misure per proteggere i dati e le risorse di rete.

Essa definirà cosa è necessario fare quando un bene viene spostato da un edificio all'altro o da un'ubicazione a un'altra. Questa politica prevede l'aggiornamento di un database di tracciamento delle risorse affinché sia nota l'ubicazione di tutte le apparecchiature informatiche.

La politica aiuterà inoltre gli amministratori della rete a proteggere la rete stessa poiché essi conosceranno la stazione nella quale sono ubicati gli utenti e i computer, ad esempio in presenza di un worm che sta infettando la rete. La presente politica prevede anche la possibilità che i dati presenti su un computer e spostati tra strutture sicure siano di natura sensibile e debbano quindi essere codificati durante il trasferimento.

3.2 Scopo e responsabilità

La presente politica è pensata per proteggere le risorse aziendali collegate alla rete definendo una politica e una procedura per il controllo delle risorse. Queste politiche contribuiranno a impedire la perdita di dati o di risorse aziendali e ridurranno il rischio di perdita di dati dovuta a una scarsa programmazione.

Il CTO è responsabile in ultima analisi delle attività di sviluppo, implementazione e attuazione di questa Politica.

3.3 Risorse tracciate

Questa sezione definisce quali risorse IT devono essere tracciate e in che misura.

3.4 Tipologie di risorse IT

Questa sezione categorizza le tipologie di risorse soggette a tracciamento.

1. Stazioni di lavoro desktop
2. Computer mobili - laptop
3. Telefoni cellulari e tablet
4. Stampanti, fotocopiatrici, fax, macchine multifunzione
5. Dispositivi palmari
6. Scanner
7. Server
8. Firewall
9. Router
10. Switch
11. Dispositivi di memoria

3.4.1 Risorse tracciate

Le risorse aventi valore commerciale inferiore alle 100 sterline (GBP), compresi componenti per computer come schede video o audio, non saranno tracciate. Tuttavia, tutte le risorse dotate di funzioni di data storage saranno tracciate, indipendentemente dal loro valore commerciale. Esse comprendono:

1. Dischi rigidi
2. Unità di storage temporaneo
3. Nastri contenenti dati, inclusi i dati di backup del sistema
4. Anche se non tracciati in modo specifico, altri dispositivi di storage come i dischi CD ROM e i floppy rientrano nel tracciamento previsto in questa Politica ai fini dello smaltimento e della conservazione sicura

3.4.2 Small Memory Devices

I piccoli dispositivi di memoria non saranno tracciati in base alla loro posizione ma alla persona cui sono stati affidati. Esse comprendono:

1. Floppy
2. Dischi CD ROM
3. Chiavette di memoria

Qualora l'uso di queste tipologie di dispositivi sia consentito ad alcuni dipendenti, la persona cui è stato affidato il dispositivo dovrà firmare un apposito documento di ricezione. Inoltre tutti i dipendenti devono accettare di gestire le chiavette di memoria, i floppy e i dischi CD ROM in modo responsabile e attenersi a queste linee guida:

1. Non salvare mai dati sensibili su tali supporti senza autorizzazione. Qualora vengano salvati dei dati sensibili su questi dispositivi, sarà necessario ottenere un permesso speciale e il dispositivo di memoria dovrà essere conservato in un luogo sicuro.
2. Non salvare mai dati dei clienti su questi supporti.
3. Non usare mai questi dispositivi per copiare programmi eseguibili dall'esterno della rete senza autorizzazione e senza prima aver scansionato il programma con un programma antivirus e antimalware approvato e aggiornato. Qualsiasi programma inserito nella rete dovrà essere precedentemente approvato dal reparto IT.

Per maggiori informazioni fare riferimento alla Politica sui supporti rimovibili.

3.5 Requisiti di tracciamento delle risorse

1. Tutte le risorse devono essere corredate da ID. Quando la risorsa viene acquisita verrà assegnato un numero di tracciamento interno, oppure nella presente Politica dovrà essere specificato l'uso dei codici ID del produttore.
2. Verrà creato un database di tracciamento delle risorse per tenere traccia delle stesse. Esso comprenderà tutte le informazioni presenti nella tabella Checklist per il trasferimento delle risorse insieme alla data della modifica della risorsa.
3. Quando viene acquisita una risorsa, si procede all'attribuzione di un'ID e nel database di tracciamento delle risorse verranno immessi i dati a essa relative

3.6 Procedura di trasferimento

3.6.1 Checklist per il trasferimento delle risorse

When an asset type listed on the Asset Types list is transferred to a Quando un tipo di risorsa riportata nell'elenco "Tipologie delle risorse" viene trasferita in una nuova sede o a un nuovo incaricato, questi deve compilare la Checklist per il trasferimento delle risorse, che verrà poi approvata da un rappresentante autorizzato dell'azienda. L'incaricato è la persona cui viene affidata la cura della risorsa. Nel caso di una postazione di lavoro, solitamente si tratta dell'utente che la utilizza più frequentemente. Nel caso di altre attrezzature, l'incaricato è la principale persona responsabile della manutenzione o della gestione dell'attrezzatura.

Questi dovrà compilare il modulo della Checklist per il trasferimento delle risorse e indicare se la risorsa è nuova, viene trasferita in una nuova ubicazione, affidata a un nuovo incaricato o se è destinata allo smaltimento. È necessario compilare i seguenti campi:

Tipologia di risorsa:

1. ID number
2. Nome della risorsa
3. Ubicazione attuale
4. Incaricato designato
5. Nuova ubicazione
6. Nuovo incaricato
7. Ubicazione dei dati sensibili

Dopo che la persona incaricata lo avrà compilato e firmato, il modulo della Checklist per il trasferimento delle risorse dovrà essere firmato anche da un rappresentante autorizzato.

3.6.2 Inserimento dei dati

Quando la Checklist per il trasferimento delle risorse sarà completa dovrà essere consegnata al responsabile del database per il tracciamento delle risorse. Quest'ultimo si accerterà che i dati contenuti nei moduli vengano inseriti nel database per il tracciamento delle risorse entro una settimana.

3.6.3 Verifica del database

I responsabili che gestiscono progetti che hanno previsto un cambio di ubicazione delle attrezzature dovranno verificare periodicamente che le risorse trasferite recentemente siano state aggiunte al database. Il database deve contenere un elenco dei trasferimenti recenti facilmente consultabile. I responsabili dovranno consultare il database su base settimanale per accertarsi che le risorse trasferite nelle ultime due o tre settimane siano state inserite.

3.7 Trasferimenti di risorse

Questa Politica si applica a qualsiasi trasferimento di risorse compresi i seguenti:

1. Acquisto di una o più risorse
2. Nuova ubicazione di una o più risorse
3. Cambio di persona incaricata delle risorse, compresi i casi di sostituzione o licenziamento.
4. Smaltimento di una o più risorse compresi:
5. Restituzione della risorsa al produttore o al rivenditore nel caso di reso in garanzia
6. Risorsa noleggiata restituita al locatore

In tutti questi casi dovrà essere compilata la Checklist per il trasferimento delle risorse.

3.8 Pulizia dei dispositivi

Quando una risorsa informatica viene trasferita a un altro soggetto incaricato, qualsiasi dato riservato presente sul dispositivo dovrà essere protetto e/o distrutto. Il metodo di distruzione dei dati dipende dal livello di sensibilità dei dati presenti sul dispositivo e da chi sarà il prossimo utente del dispositivo (all'interno e sotto il controllo dell'azienda o al di fuori di questa).

3.9 Smaltimento delle risorse

Il tema dello smaltimento delle risorse è importante in quanto durante o prima di questo passaggio il dispositivo in questione dovrà essere ripulito di tutti i dati sensibili in esso contenuti. Il responsabile dell'utente del dispositivo dovrà determinare il livello di sensibilità massima dei dati archiviati sul dispositivo stesso. Di seguito riportiamo l'intervento da realizzare sul dispositivo in base al livello di sensibilità dei dati secondo il corrispondente processo di valutazione dei dati.

1. Nessuno (dati non classificati) - Nessun requisito di cancellazione dei dati ma, a fini prudenziali, si procede normalmente alla cancellazione dei dati utilizzando qualsiasi mezzo come la sanificazione elettronica, la distruzione fisica o la smagnetizzazione.
2. Livello basso (dati sensibili) - Cancellazione dei dati utilizzando qualsiasi mezzo come la sanificazione elettronica, la distruzione fisica o la smagnetizzazione.
3. Livello medio (dati riservati) - I dati devono essere cancellati utilizzando una tecnologia approvata per accertarsi che non siano leggibili utilizzando tecniche speciali altamente sofisticate.
4. Livello alto (dati segreti) - I dati devono essere cancellati utilizzando una tecnologia approvata per accertarsi che non siano leggibili utilizzando tecniche speciali altamente sofisticate. Le tecnologie approvate dovranno essere specificate in una Procedura di rimozione dei dati dai supporti in base alla tipologia di risorsa, compresi:

    1. Floppy
    2. Chiavette di memoria
    3. Dischi CD ROM
    4. Nastri
    5. Hard drive
    6. Memorie RAM
    7. Memorie ROM o dispositivi con memoria ROM

3.10 Utilizzo dei supporti

La presente Politica definisce le tipologie di dati che possono essere archiviati sui supporti rimovibili e se tali supporti possano essere rimossi da una struttura fisicamente sicura e in quali condizioni ciò sia consentito. I supporti rimovibili comprendono:

1. Floppy
2. Dischi di memoria
3. Dischi CD ROM
4. Nastri

Di seguito riportiamo la politica applicabile al dispositivo in base al livello di sensibilità dei dati archiviati sul dispositivo stesso secondo il processo di valutazione dei dati.

1. Dati non classificati – I dati possono essere rimossi con l'approvazione di un responsabile di primo livello e l'autorizzazione ha carattere perpetuo per la durata del rapporto di impiego del dipendente, tranne in caso di revoca. Il dispositivo può essere inviato ad altre sedi utilizzando qualsiasi vettore pubblico o privato.
2. Dati sensibili – I dati possono essere rimossi dalle aree sicure solo previa autorizzazione di un dirigente o di un responsabile di livello superiore e l'autorizzazione vale una sola volta.
3. Dati riservati – I dati possono essere rimossi dalle aree sicure solo con l'autorizzazione del Vice Presidente o di un responsabile di livello superiore. Sia per il metodo di trasferimento che in fase di arrivo devono essere predisposte precauzioni specifiche, adeguatamente documentate.
4. Dati segreti – I dati possono essere rimossi dalle aree sicure solo con l'autorizzazione del Presidente o di un responsabile di livello superiore. Sia per il metodo di trasferimento che in fase di arrivo devono essere predisposte precauzioni specifiche, adeguatamente documentate.
5. Dati della massima segretezza – I dati non possono in nessun caso essere rimossi dalle aree sicure.

3.11 Dispositivi di proprietà dei dipendenti

La presente Politica definisce le tipologie di dispositivi di proprietà dei dipendenti che possono essere utilizzati da questi ultimi negli ambienti aziendali.

1. I telefoni cellulari personali possono essere usati in azienda, ma non devono essere collegati tramite Wi-Fi alla rete aziendale.
2. Non è consentito l'uso di nessun altro dispositivo di proprietà dei dipendenti nelle sedi dell'azienda e nessun altro dispositivo potrà essere collegato alla rete cablata o Wi-Fi dell'azienda.

3.12 Implementazione

Poiché la sicurezza e l'integrità dei dati, insieme alla protezione delle risorse, è essenziale per l'operatività dell'azienda, i dipendenti che non rispettino questa politica potranno essere soggetti a misure disciplinari fino al licenziamento. Qualsiasi dipendente che venga a conoscenza di una violazione della presente Politica è tenuto a comunicarlo al proprio superiore o a un altro rappresentante autorizzato.

3.13 Formazione dei dipendenti e accettazione della Politica

Ogni dipendente dell'azienda è tenuto a conoscere le politiche e le procedure in vigore relativamente alla sicurezza IT e dovrà svolgere la necessaria formazione, almeno una volta all'anno. I dipendenti dovranno inoltre firmare un documento di accettazione in cui dichiarano di conoscere la Politica e di impegnarsi a rispettarne le prescrizioni.

4. Politica sui supporti rimovibili

4.1 Panoramica generale

I supporti rimovibili sono una fonte nota di infezioni da malware e in molte aziende sono stati direttamente correlati alla perdita di informazioni sensibili.

4.2 Scopo

Lo scopo di questa Politica è ridurre al minimo il rischio di perdita o esposizione dei dati sensibili da noi detenuti e ridurre il rischio di infezioni da malware sui computer da noi gestiti.

4.3 Ambito

La presente Politica concerne tutti i computer e i server utilizzati nella nostra azienda.

4.4 Politica

I nostri dipendenti potranno utilizzare esclusivamente supporti rimovibili di nostra proprietà nei propri computer di lavoro. I nostri supporti rimovibili non potranno essere collegati o utilizzati nei computer che non siano di proprietà o che non siano stati noleggiati dalla nostra azienda senza espressa autorizzazione da parte del team incaricato della sicurezza.

I dati sensibili dovranno essere archiviati su supporti rimovibili esclusivamente se strettamente necessario all'esecuzione delle proprie mansioni o per fornire i dati su richiesta di altre agenzie statali o federali. I dati dei clienti non dovranno essere mai archiviati sui supporti rimovibili.

Sarà possibile richiedere di volta in volta l'applicazione di eccezioni a questa Politica, le quali saranno soggette ad approvazione da parte del team incaricato della sicurezza.

4.5 Conformità alla Politica

4.5.1 Gestione della conformità

Il team incaricato della sicurezza verificherà la conformità alla presente Politica attraverso vari metodi, compresi in via non limitativa: ispezioni fisiche periodiche, report degli strumenti di business, audit interni ed esterni e feedback da parte del titolare della Politica.

4.5.2 Eccezioni

Eventuali eccezioni alla Politica dovranno essere precedentemente approvate dal team incaricato della sicurezza.

4.5.3 Non conformità

Qualora un dipendente violi la presente Politica, potrà essere sottoposto ad azione disciplinare, che potrebbe culminare nella risoluzione del rapporto di lavoro.

5. Politica su virus e codici nocivi

5.1 Panoramica generale

Questa Politica e procedura concerne la gestione di virus e codici nocivi.

5.2 Scopo

Lo scopo di questa Politica è illustrare l'approccio da adottare all'interno della nostra azienda per evitare virus e codici nocivi e cosa fare in caso di infezione.

5.3 Ambito

La presente Politica concerne tutti i computer e i server utilizzati nella nostra azienda.

5.4 Politica

Dato che gli aggressori informatici stanno passando da attacchi che recano un semplice danno o la distruzione ad attività motivate dal guadagno economico, gli attacchi con codice nocivo sono divenuti più sofisticati e rappresentano una reale preoccupazione per le aziende. Un attacco tramite codice nocivo su larga scala, spesso definito "outbreak" o "epidemia", può causare vasti danni e interruzioni dei servizi in un'azienda, oltre a richiedere lunghi tempi e molte energie per il ripristino delle normali attività. È quindi essenziale adottare misure preventive adeguate come l'implementazione di strumenti di protezione e rilevamento, per salvaguardare un'azienda da attacchi di codice nocivo.

Tuttavia nel mondo della sicurezza informatica non esiste la protezione totale. È importante anche che l'azienda sviluppi una solida procedura nei casi di incidenti di sicurezza informatica affinché il personale sia meglio preparato a gestire tali "outbreak" di codice nocivo in modo più organizzato, efficiente ed efficace.

Un processo di risposta a un incidente informatico deve prevedere tre fasi: “Pianificazione e preparazione”, “Risposta” e “Conseguenze”. Questa sezione illustra le fasi di “Risposta” e “Conseguenze”, importanti per una buona gestione di un “outbreak” di codice nocivo. Per maggiori informazioni sul passaggio “Pianificazione e preparazione”, fare riferimento alla sezione “Gestione degli incidenti di sicurezza dell’azienda” della Politica.

Il passaggio “Risposta” comprende i cinque punti seguenti: Escalation

- Rilevazione e identificazione
- Escalation
- Contenimento
- Eliminazione
- Recovery

5.4.1 Rilevazione e identificazione

5.4.1.1 Determinare in modo esaustivo se si è verificato l’“outbreak” di codice nocivo

L’obiettivo di questo passaggio è determinare se si è verificato un “outbreak” di codice nocivo. Gli indicatori tipici di “outbreak” di codice nocivo sono:

- Gli utenti si lamentano della lentezza dell'accesso a Internet, dell’esaurimento delle risorse del sistema, di un accesso rallentato ai dischi o di avviamenti lenti del sistema.
- Un sistema HIDS (Host-based Intrusion Detection System) o un software antivirus o per il rilevamento di codice nocivo ha generato vari alert
- Vi è un aumento significativo dell’uso della rete.

- I log dei router o dei firewall perimetrali hanno registrato una serie di violazioni di accesso.
- È stato rilevato un picco di traffico SMTP prodotto da indirizzi IP interni.
- Sono stati rilevati numerosi tentativi di Port-Scan e connessione falliti.
- L'amministratore di sistema nota una deviazione anomala dai normali flussi di traffico di rete.
- Gli strumenti di controllo della sicurezza come il software antivirus e i firewall personali sono stati disattivati su numerosi host.
- Instabilità generale e blocchi del sistema.

Una volta rilevate una o più delle condizioni sopra indicate, il personale IT dovrà controllare e convalidare immediatamente tutte le attività sospette per determinare se si è verificato un "outbreak". Una volta confermata la violazione della sicurezza con codice nocivo, è importante raccogliere informazioni su tale codice, passaggio essenziale per il processo di contenimento ed eliminazione.

Le informazioni sul codice nocivo possono essere recuperate tramite i siti web dei fornitori del software antivirus qualora il codice nocivo sia attivo da tempo, analizzando gli alert del software antivirus e di rilevazione del codice nocivo, esaminando i file di log di firewall e router. Le seguenti domande possono contribuire a identificare le caratteristiche del codice nocivo:

- Di quale tipo di codice nocivo si tratta (worm di rete, worm di mass-mailing, virus o trojan horse, ecc.)?
- In che modo si propaga il codice nocivo (attaccando servizi di rete vulnerabili? Tramite mass-mailing?)

- Se il codice nocivo si propaga attaccando un sevizio vulnerabile, qual è la vulnerabilità che viene sfruttata? È stata rilasciata una patch per risolvere la vulnerabilità? Quali sono i servizi o le porte oggetto dell'attacco?
- Il codice nocivo inserisce delle backdoor nel sistema infetto?
- In che modo è possibile eliminare il codice nocivo dal sistema infetto? Sono disponibili strumenti per la sua eliminazione?

5.4.1.2 Esecuzione di valutazioni preliminari

Una volta identificato un “outbreak”, il personale IT deve valutare l’ambito, il danno e l’impatto dell'evento per gestirlo in modo efficace.

5.4.1.3 Registrazione di tutti gli interventi

Il personale dovrà registrare tutti gli interventi per gestire l’“outbreak” e i risultati corrispondenti. Ciò può agevolare l’identificazione dell’evento e la sua valutazione, oltre a fornire prove per eventuali procedimenti penali e altre informazioni utili per le fasi successive di gestione dell’incidente. Durante l’intero processo di risposta all’incidente di sicurezza è necessario realizzare dei log degli interventi.

5.4.1.4 Contenimento

Il terzo passaggio della risposta a un attacco di codice nocivo è il contenimento. Riportiamo di seguito le attività che è necessario svolgere nella fase di contenimento:

5.4.1.5 Identificazione dei sistemi infetti

Identificare in modo chiaro i sistemi infetti è sempre la prima cosa da fare nella fase di contenimento. Sfortunatamente si tratta di un processo molto complesso per via della natura dinamica dell'attuale ambiente IT. Di seguito riportiamo alcuni suggerimenti che possono contribuire a identificare i sistemi infetti in un ambiente gestito:

- Realizzare un'accurata scansione dei virus su tutti i sistemi applicando le ultime signature disponibili, e gli strumenti di riparazione e rilevazione dei virus. Dato che nessun software antivirus o strumento di rilevazione di codice nocivo può da solo rilevare tutte le tipologie di minacce, può essere necessario utilizzare più strumenti di scansione antivirus per garantire che vengano rilevati tutti i codici nocivi.
- Rivedere tutti i file di log di router e firewall.
- Fornire agli utenti istruzioni su come identificare le infezioni.
- Configurare gli strumenti IPS o IDS per identificare le attività associate alle infezioni.
- Eseguire periodicamente attività di packet-sniffing per rilevare il traffico di rete rispondente alle caratteristiche di un codice nocivo.

5.4.1.6 Contenimento di un "outbreak"

Il contenimento dell "outbreak" può essere svolto in diversi modi. Di seguito riportiamo le tattiche più comuni:

- Utilizzando strumenti automatizzati
  Il contenimento della diffusione del codice nocivo può essere realizzato con strumenti automatizzati come i software antivirus o gli strumenti di rilevazione del codice nocivo, IDS e IPS. Se il codice nocivo non viene rilevato dai sistemi di protezione antivirus esistenti, anche applicando le ultime signature disponibili, è necessario richiedere l'assistenza di fornitori di software antivirus per creare una nuova signature del codice nocivo.
- Disattivando la connessione
  Un "outbreak" di codice nocivo può essere contenuto in modo efficace scollegando rapidamente i sistemi infetti dall'infrastruttura generale di rete. Ciò può essere realizzato applicando i controlli di accesso sui dispositivi di rete o scollegando fisicamente i cavi di rete. In alcuni casi per contenere la diffusione del codice nocivo ad altri rami aziendali, può essere necessario scollegare temporaneamente i segmenti della rete coinvolti dalla dorsale di rete. Tuttavia questa strategia di contenimento avrà sicuramente conseguenze sul funzionamento degli altri sistemi non infetti del segmento.
- Disattivando i servizi
  Il codice nocivo può propagarsi attraverso i servizi di rete, ad esempio le unità condivise di una rete. Il blocco temporaneo o addirittura l'interruzione dei servizi di rete utilizzati dai codici nocivi possono contribuire a contenere gli incidenti.

- Eliminando la vulnerabilità
  Il codice nocivo può diffondersi attaccando i servizi di rete vulnerabili. Gestendo tali vulnerabilità utilizzate dal codice nocivo, tramite ad esempio l'applicazione di patch di sicurezza sui sistemi più esposti, i canali di propagazione possono essere eliminati, contenendo di conseguenza la diffusione. Inoltre, anche alcune cattive configurazioni - come i controlli di accesso deboli sulle unità condivise di rete - possono essere sfruttate dal codice nocivo. Correggendo eventuali configurazioni scorrette è possibile contenere il codice nocivo.
- Tramite la partecipazione degli utenti
  La partecipazione degli utenti è essenziale nel processo di contenimento in un ambiente in cui solo un numero limitato di personale addetto all'assistenza tecnica è disponibile per gestire un "outbreak", ad esempio in sedi minori remote o in ambienti d'ufficio non gestiti. Gli utenti devono ricevere istruzioni chiare su come identificare le infezioni e quali misure occorra adottare in presenza di un'infezione confermata, come il lancio degli strumenti di rimozione antivirus sul sistema colpito.

5.4.1.7 Registrazione di tutti gli interventi svolti

È importante mantenere una documentazione ben organizzata di tutti gli interventi svolti in questa fase poiché alcune misure di contenimento potrebbero richiedere modifiche temporanee alla configurazione o alle impostazioni dei sistemi e dell'infrastruttura di rete. Tali modifiche dovranno essere rimosse dopo l'evento.

È importante comprendere che l'arresto dell'infezione causata dal codice nocivo non impedisce necessariamente ulteriori danni ai sistemi infetti. Ad esempio, l'infezione può essere contenuta disattivando la connessione di rete, ma il codice nocivo può restare attivo e cancellare file sul sistema infetto.

Quindi occorre attuare un processo di eliminazione totale appena possibile o parallelamente al processo di contenimento.

5.4.2 Eliminazione

L'eliminazione di una "'outbreak" di codice nocivo deve essere strutturata in modo da rimuovere il codice nocivo da tutti i sistemi e supporti infetti, e correggere la causa dell'infezione. Prima di realizzare la procedura di eliminazione, è consigliabile raccogliere tutte le informazioni necessarie, compresi i file di log, che potrebbero essere eliminati o ripristinati durante la procedura di pulizia, e che possono essere utili per l'analisi successiva.

Come strumento primario di eliminazione, solitamente si ricorre al software di scansione del codice nocivo o antivirus e agli strumenti di rimozione.

Tuttavia in alcuni casi può essere necessario ricostruire da zero i sistemi infetti. Ad esempio, se il codice nocivo ha scaricato e ha creato una backdoor sui sistemi infetti, la ricostruzione totale può essere la scelta più sicura per ripristinare l'integrità dei sistemi. La ricostruzione di un sistema solitamente comprende i seguenti interventi:

- Reinstallare il sistema partendo da una fonte affidabile come un disco di installazione o un'immagine di sistema pulita e affidabile.

- Mettere al sicuro i sistemi appena installati, controllando e accertandosi che su ogni macchina siano stati applicati: le signature più aggiornate dei virus, gli strumenti di rilevazione e riparazione antivirus e tutte le patch di sicurezza necessarie.
- Ripristinare i dati da supporti di backup puliti e noti.

5.4.3 Recovery

Ovviamente lo scopo principale della fase di recovery è il ripristino di tutti i sistemi affinché sia possibile tornare al normale funzionamento. In presenza di un "outbreak" di codice nocivo, il ripristino delle funzionalità e dei dati sui sistemi infetti può essere già stato effettuato nell'ambito del processo di eliminazione. Oltre a ripristinare i sistemi infetti, la rimozione delle eventuali misure provvisorie di contenimento - come la sospensione delle connessioni di rete - è un altro aspetto importante della procedura di ripristino.

Prima della rimozione delle misure di contenimento, un passaggio importante è la valutazione del rischio di sicurezza prima dell'intervento in modo da garantire che non vengano rilevate infezioni e che la causa dell'infezione iniziale sia stata corretta.

Tutte le parti coinvolte riceveranno apposita comunicazione prima del ripristino dei servizi sospesi. Il personale IT dovrà ripristinare funzionalità e server specifici fase per fase, in modo controllato, e in ordine di richiesta, ad esempio partendo dai servizi essenziali o da quelli che interessano la maggioranza degli utenti. Dopo aver ripristinato i servizi sospesi, è importante verificare che il ripristino sia andato a buon fine e che tutti i servizi siano tornati alla normale operatività. Potranno essere attuate ulteriori misure di monitoraggio per controllare eventuali attività sospette nei segmenti della rete coinvolti.

5.4.4 Conseguenze

Il ripristino dei sistemi infetti non determina la fine di un "outbreak" di codice nocivo. È importante anche mettere in atto le necessarie azioni di follow-up. Esse possono comprendere una valutazione completa dei danni causati, la messa a punto del sistema per impedire che il problema possa ripresentarsi, gli aggiornamenti alle politiche e alle procedure di sicurezza, e l'analisi del caso per valutare la possibilità di un procedimento penale. Le attività in questa fase possono comprendere quanto segue:

- Rivedere l'efficacia delle procedure e dei meccanismi esistenti per la protezione dai codici nocivi e dai virus compreso il controllo e la gestione centralizzati della distribuzione delle signature dei virus e l'aggiornamento dei motori di rilevamento e riparazione, la scansione periodica programmata dei virus, ecc.
- Aggiornare politiche, linee guida e procedure applicabili, quando necessario.
- Attuare le nuove misure di sicurezza introdotte nelle revisioni di politica/linee guida/procedure per proteggere i sistemi da attacchi futuri.

- Ricordare agli utenti di attenersi alle migliori prassi di sicurezza come ad esempio non aprire i messaggi e-mail provenienti da mittenti sconosciuti/sospetti, aggiornare le patch di sicurezza e le definizioni dei virus regolarmente e ogniqualvolta sia necessario, ecc.

6. Procedura di gestione degli incidenti

6.1 Scopo

Lo scopo di questa Politica è garantire un rapido rilevamento degli eventi di sicurezza e dei punti deboli, nonché reagire e rispondere in modo tempestivo agli incidenti di sicurezza.

6.2 Ambito e utenti

La presente Politica si applica all'intero ambito ISMS (Information Security Management System) ovvero a tutti i dipendenti e alle altre risorse impiegate nell'ambito dell'ISMS nonché ai fornitori e agli altri soggetti esterni all'azienda che vengono a contatto con i sistemi e i dati nell'ambito dell'ISMS.

Gli utenti di questa Politica sono tutti i nostri dipendenti, nonché tutti i soggetti sopra citati.

6.3 Riferimento

- ISO/IEC 27001, clausole A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- ISO/IEC 27001, clausole 16.1.1, 16.1.2, 16.1.7, e 18.1.2

6.4 Politica

Un incidente correlato alla sicurezza dei dati è “un singolo evento o una serie di eventi inattesi o indesiderati che coinvolgono la sicurezza dei dati e che hanno una forte probabilità di compromettere le attività aziendali nonché di minacciare la sicurezza dei dati stessi” (ISO/IEC 27000:2009).

6.4.1 Politica

Un incidente correlato alla sicurezza dei dati è “un singolo evento o una serie di eventi inattesi o indesiderati che coinvolgono la sicurezza dei dati e che hanno una forte probabilità di compromettere le attività aziendali nonché di minacciare la sicurezza dei dati stessi” (ISO/IEC 27000:2009).

6.4.2 Procedura da adottare in presenza di punti deboli o eventi correlati alla sicurezza

La persona che è stata informata su un punto debole o un evento correlato alla sicurezza analizza le informazioni, stabilisce la causa e - se necessario - suggerisce interventi preventivi e correttivi.

Nei casi in cui siano coinvolti servizi online o dati personali dei clienti, l’incaricato della sicurezza dovrà decidere se i clienti, a cui fanno riferimento i i punti deboli o gli eventi correlati alla sicurezza, debbano essere informati (qualora il cliente non sia la persona che ha redatto il report iniziale sull'evento). Qualora si decida di informare i clienti, le notifiche dovranno avvenire quanto prima, telefonicamente o di persona, secondo le procedure definite.

6.4.3 Gestione degli incidenti di minore entità

Qualora venga rilevato un incidente di minore entità, la persona che ha ricevuto la comunicazione a riguardo, coordinandosi con il personale del cliente e ove necessario o richiesto, dovrà adottare la seguente procedura:

1. Adottare le misure necessarie a contenere l'incidente.
2. Analizzare la causa dell'incidente..
3. Adottare le misure correttive per eliminare la causa dell'incidente.
4. Informare le persone coinvolte nonché l'incaricato della sicurezza in merito alla procedura adottata per la gestione dell'incidente.

La persona che ha ricevuto comunicazione di un incidente di minore entità deve registrare l'incidente fornendo notifica via e-mail all'incaricato della sicurezza, e inserire un difetto in Jira per avvisare il team di sviluppo.

6.4.4 Gestione degli incidenti di maggiore entità

In caso di incidenti gravi che potrebbero causare interruzione delle attività per un periodo di tempo inaccettabile, sarà svolta una delle seguenti procedure:

In orario di lavoro:

1. Viene indetta una riunione di emergenza del team incaricato della sicurezza
2. L'incidente viene sottoposto a valutazione in termini di sicurezza e gravità
3. Viene presa una decisione sulle misure da adottare
4. Vengono messe in atto le misure previste
5. Non appena possibile viene svolta e rivista dal team un'analisi sulla causa dell'incidente

Al di fuori dell'orario di lavoro:

1. La prima persona che riceve notifica dell'incidente convoca le risorse tecniche che riesce a reperire
2. L'incidente viene sottoposto a valutazione in termini di sicurezza e livello di gravità, nonché per capire se il tentativo di risolvere temporaneamente il problema possa causare maggiori danni in assenza delle risorse giuste
3. Viene presa una decisione sulle misure da adottare
4. Vengono realizzati gli interventi minimi
5. In orario lavorativo viene svolta una valutazione più dettagliata con interventi ulteriori, se necessario
6. Non appena possibile viene svolta e rivista dal team un'analisi sulla causa dell'incidente

6.4.5 Apprendere dagli incidenti

Il team incaricato della sicurezza deve rivedere tutti gli incidenti di minore entità ogni tre mesi e inserire nell'apposito log quelli ricorrenti o quelli che in una successiva occasione potrebbero trasformarsi in incidenti di maggiore entità.

Il team incaricato della sicurezza deve analizzare ogni incidente registrato nell'apposito log (identificando tipologia, correlazione e costo dell'incidente) e, se necessario, suggerire azioni preventive o correttive.

6.4.6 Azioni disciplinari

Insieme al reparto HR, l'incaricato della sicurezza deve invocare una procedura disciplinare per ogni violazione del regolamento sulla sicurezza.

6.4.7 Raccolta di prove

Il team incaricato della sicurezza definirà le regole per identificare, raccogliere e conservare le prove che saranno accettate in procedimenti legali e di altro tipo.

Nelle situazioni che coinvolgono dati personali identificativi del cliente, l'incaricato della sicurezza definirà insieme al cliente del servizio cloud la procedura per identificare, raccogliere e conservare le prove che saranno accettate in successivi procedimenti legali e di altro tipo.

6.5 Gestione dei record in base al presente documento

Nome del record	Ubicazione	Responsabile archiviazione	Controlli per la protezione del record	Tempo di conservazione
Log degli incidenti	DropBox Azure	Team incaricato della sicurezza	Solo i membri del team hanno diritto di modificare il log	5 anni
Regolamento per identificare, raccogliere e conservare le prove	DropBox Azure	Incaricato della sicurezza	Solo l'incaricato della sicurezza ha il diritto di modificare e pubblicare il regolamento	I record vengono conservati per un periodo di 5 anni

Solo l'incaricato della sicurezza può concedere ad altri dipendenti l'accesso ai record.

6.6 Validità e gestione dei documenti

Il presente documento ha validità a partire dal 5 ottobre 2017.

Il titolare di questo documento è l'incaricato della sicurezza, il quale dovrà controllare e - se necessario - aggiornare il documento almeno ogni sei mesi.

Nella valutazione dell'efficacia e dell'adeguatezza di questo documento, dovranno essere considerati i seguenti criteri:

- Numero di punti deboli o incidenti non comunicati alle persone autorizzate
- Numero di incidenti non gestiti nel modo più adeguato
- Numero di incidenti non registrati nell'apposito log
- Numero di incidenti per i quali le prove necessarie a intraprendere azioni legali non sono state adeguate
- Numero di violazioni dei regolamenti sulla sicurezza in cui non è stata invocata alcuna procedura disciplinare

Le precedenti versioni di questa procedura devono essere conservate per un periodo di 5 anni, tranne ove diversamente specificato da un requisito legale o contrattuale.

7. Politica di backup

7.1 Scopo

Lo scopo di questo documento è garantire che a intervalli predefiniti vengano create delle copie di backup, periodicamente testate.

7.2 Ambito e utenti

Il presente documento si applica all'intero ambito ISMS (Information Security Management System) ovvero a tutta la tecnologia informatica e di comunicazione che rientra nell'ambito definito.

Gli utenti di questo documento sono i nostri dipendenti.

7.3 Riferimento

- ISO/IEC 27001 standard, clause A.12.3.1

7.4 Politica

7.4.1 Procedura di backup

Per tutti i sistemi software, dati e video è necessario creare delle copie di backup.

La creazione di backup è un processo automatizzato ed è parte integrante dei sistemi software scritti e implementati da noi. Il responsabile DevOps ha, in ultima analisi, l'incarico di garantire che i backup siano effettuati e conservati correttamente.

Quando viene realizzata la copia di backup, i log della procedura di backup vengono creati automaticamente sui sistemi.

Il software di sistema viene salvato in una serie di repository e utilizza Git, consentendo di tornare a versioni precedenti nell'ambito del sistema.

I dati vengono automaticamente replicati in database slave su altri server, ubicati in altri data centre. I backup binari vengono realizzati ogni ora e archiviati su Amazon S3. I backup notturni avvengono giornalmente e sono archiviati su Amazon S3.

I video vengono duplicati su Amazon S3 non appena sono elaborati. Restano sul server primario e S3 per almeno 5 giorni. Una volta cancellati dal server primario, vengono conservati solo su S3. S3 è comunque configurato per offrire un'elevata ridondanza.

7.4.2 Test delle copie di backup

Il repository del sistema software viene testato giornalmente mentre gli sviluppatori vi lavorano.

I backup dei dati vengono testati quotidianamente mentre il backup viene ripristinato su un server di staging che agisce come parte del processo di deployment.

I backup dei contenuti video vengono testati continuamente; i video vengono riprodotti dal sistema di backup dopo il periodo iniziale di 5 giorni e uno script delle anomalie evidenzia eventuali video che non sono stati copiati nel backup S3.

7.4.3 Gestione degli archivi in base alla presente politica

Il repository del sistema software viene testato giornalmente mentre gli sviluppatori vi lavorano.

Nome del record	Ubicazione	Responsabile archiviazione	Controlli per la protezione del record	Tempo di conservazione
Log della procedura di backup - formato elettronico	Sistema che esegue la procedura di backup	Responsabile DevOps	I log sono di sola lettura, non possono essere cancellati né modificati	I log vengono conservati per un periodo di 2 anni

7.4.4 Validità e gestione dei documenti

Il presente documento ha validità a partire dal 5 ottobre 2017.

Il titolare di questo documento è il CTO, il quale dovrà controllare e - se necessario - aggiornare il documento almeno ogni anno.

Nella valutazione dell'efficacia e dell'adeguatezza di questo documento, dovranno essere considerati i seguenti criteri:

Numero di test di backup falliti

Le precedenti versioni di questa politica devono essere conservate per un periodo di 5 anni, tranne ove diversamente specificato da un requisito legale o contrattuale.

Allegato

I. Informazioni sul team incaricato della sicurezza

Il team incaricato della sicurezza comprende, come requisito minimo, i seguenti ruoli:

- Responsabile del consiglio incaricato dello sviluppo e della sicurezza (CTO)
- CISO (Chief Information Security Officer)
- CSA (Chief Software Architect)
- Responsabile DevOps
- Responsabile dello sviluppo

Il team deve incontrarsi su base mensile.

Il team analizzerà gli incidenti registrati nel mese precedente, compresi eventuali report post mortem dell'incidente, e raccomanderà le modifiche in termini di sistema, prassi, procedure o politiche.

Il team analizzerà gli incidenti in base a un elenco di clienti e, qualora qualcuno risulti coinvolto, contatterà il cliente o i clienti in questione secondo le modalità definite.

II. Log degli incidenti

Gli incidenti vengono classificati nelle seguenti tipologie:

- ollegati ai dati (direttamente correlati a tecnologie informatiche o di comunicazione)
- N on collegati ai dati (tutti gli altri)

Informazioni sugli incidenti:

Il log degli incidenti è un documento di Google.

N.	Data dell'incidente	Breve descrizione (nome) dell'incidente	Person responsible for handling the incident	Descrizione dettagliata - conseguenze, durata, sistemi /dati interessati dall'incidente, ecc.	Costi [in valuta locale] - diretti e indiretti	Riferimento al modulo di misura correttiva
1						
2						
3						