EDISOFT S.r.l.
SISTEMI INFORMATICI - WEB - SOFTWARE

PIANO ADEGUAMENTO PROTOCOLLO DORA

LINEE GUIDA VERSO LA CONFORMITÀ ALLA NORMATIVA

Il presente documento delineerà l'approccio, l'ambito di applicazione e le attività necessarie per l'adeguamento al Protocollo DORA (Regolamento (UE) 2022/2554), fornendo una panoramica chiara delle misure da adottare per garantire la conformità normativa. Inoltre, definirà il modello di gestione dei rischi, evidenziando le strategie e le procedure da implementare per rafforzare la sicurezza e mitigare le vulnerabilità.

Edisoft Srl | P.IVA 02347420040
Corso Francia 239, Cuneo CN | Via Bodoni 23/25, Saluzzo CN | Vico Carmagnola 7/14C, Genova GE
info@edisoft.net | 0171 1836406 | www.edisoft.net

Sommario

Introduzione al progetto di consulenza

Edisoft Srl propone un servizio di consulenza specializzato per supportare le organizzazioni nell'adeguamento al Digital Operational Resilience Act (DORA), introdotto dal Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022. Il DORA stabilisce un quadro normativo armonizzato per garantire che tutte le entità del settore finanziario e i fornitori di servizi ICT critici mantengano un elevato livello di resilienza operativa digitale. L'obiettivo è quello di assicurare la continuità e la sicurezza dei servizi essenziali anche in caso di incidenti informatici o eventi avversi.

La normativa impone alle istituzioni finanziarie e ai loro fornitori obblighi stringenti in materia di gestione del rischio ICT, gestione degli incidenti, test di resilienza operativa, gestione della catena di fornitura ICT e condivisione delle informazioni relative alle minacce. L'adeguamento al DORA richiede un approccio metodico e strutturato per identificare le vulnerabilità, definire misure di mitigazione e garantire la continuità operativa.

Edisoft Srl si propone come partner strategico per accompagnare le aziende durante l'intero percorso di conformità, dalla fase di assessment fino al monitoraggio continuo delle procedure. L'approccio adottato è basato sull'ascolto attivo delle esigenze del cliente e su un'analisi approfondita dei processi aziendali, che consente di elaborare piani d'azione personalizzati. Durante tutto il percorso, le aziende saranno seguite da un team dedicato di esperti in compliance e cybersecurity, con competenze trasversali per affrontare le diverse sfide poste dalla normativa.

La normativa è parte integrante della strategia dell'UE per la finanza digitale e punta a garantire la continuità operativa dei servizi finanziari, anche in presenza di incidenti ICT significativi.

Il DORA stabilisce requisiti tecnici e organizzativi per mitigare i rischi derivanti dall'utilizzo di tecnologie digitali. Gli ambiti principali di intervento sono:

- Gestione del rischio ICT e governance
- Segnalazione e risposta agli incidenti
- Test di resilienza operativa digitale
- Gestione del rischio di terze parti
- Condivisione delle informazioni (raccomandata ma non obbligatoria)

Un elemento distintivo della nostra consulenza è l'integrazione con Formalize, una piattaforma digitale all'avanguardia che permette di centralizzare la gestione della documentazione, monitorare l'avanzamento delle attività e garantire una conformità costante e aggiornata. Grazie a Formalize, i clienti possono accedere a una dashboard dedicata per visualizzare i rischi analizzati, le attività in corso e le scadenze, ottimizzando i tempi di gestione e garantendo la trasparenza dei processi.

Ambito di Applicazione del Protocollo DORA

Il Regolamento DORA si applica a un ampio spettro di entità operative nel settore finanziario e ai fornitori di servizi ICT che supportano tali istituzioni. Il suo obiettivo è garantire che tutti gli attori coinvolti nella catena dei servizi finanziari adottino misure adeguate per prevenire, gestire e rispondere efficacemente ai rischi legati alle tecnologie digitali.

Soggetti Coinvolti

Le categorie di organizzazioni soggette al DORA includono:

- Istituti di credito e banche
- Società di investimento e gestori di fondi
- Imprese di assicurazione e riassicurazione
- Fornitori di servizi di pagamento e di moneta elettronica
- Organismi di compensazione e depositari centrali di titoli
- Fornitori terzi di servizi ICT (inclusi cloud service provider e software house)

Servizi e Attività Interessate

Il regolamento si applica a tutte le funzioni operative digitali considerate critiche per l'erogazione dei servizi finanziari, tra cui:

- Sistemi di pagamento elettronico
- Piattaforme di trading e di gestione degli investimenti
- Infrastrutture IT per la comunicazione e lo scambio dati
- Applicazioni per la gestione dei clienti e dei servizi post-vendita
- Processi di outsourcing e gestione di terze parti tecnologiche

Principio di Proporzionalità

Il DORA adotta un approccio proporzionale, modulando gli obblighi in base alla dimensione, alla complessità e alla natura dei servizi offerti dall'organizzazione. Le piccole entità saranno soggette a requisiti meno onerosi rispetto alle grandi istituzioni sistemiche. Questa flessibilità consente alle imprese di implementare misure adeguate senza incorrere in oneri eccessivi, garantendo comunque un elevato standard di sicurezza operativa.

Esclusioni e Limitazioni

Alcune organizzazioni di dimensioni ridotte o con attività marginali nel settore finanziario possono essere esentate da determinati obblighi, previa valutazione delle autorità di vigilanza competenti. Tuttavia, resta fondamentale per tutte le entità valutare attentamente la propria esposizione ai rischi ICT e adottare le misure preventive necessarie.

Perché scegliere Edisoft Srl

Scegliere Edisoft Srl significa affidarsi a un partner competente, proattivo e orientato alla concretezza. La nostra proposta va oltre la semplice conformità normativa: ci impegniamo a costruire percorsi che portino valore aggiunto all'organizzazione, migliorando i processi interni e la gestione dei rischi ICT in modo duraturo.

- **Team multidisciplinare:** I nostri esperti combinano competenze in compliance, cybersecurity e risk management per offrire un servizio completo e aggiornato.
- **Soluzioni su misura:** Ogni progetto è personalizzato in base alle esigenze specifiche, al settore e alla dimensione dell'organizzazione.
- **Tecnologia al servizio della compliance:** L'utilizzo della piattaforma Formalize consente una gestione snella, tracciabile e sempre conforme della documentazione.
- **Supporto continuo:** Garantiamo la nostra presenza in tutte le fasi, dall'assessment iniziale fino al monitoraggio successivo all'implementazione.
- **Approccio proattivo e pratico:** Identifichiamo i rischi in modo tempestivo e forniamo soluzioni operative facilmente attuabili.

Approccio alla Consulenza

Affrontare la conformità DORA richiede più di un semplice adeguamento normativo: è fondamentale adottare una strategia integrata che tenga conto della realtà operativa dell'organizzazione e delle specificità del settore. Edisoft Srl si distingue per un approccio consulenziale orientato alla collaborazione, alla praticità e alla personalizzazione. Non ci limitiamo a fornire indicazioni teoriche: accompagniamo i nostri clienti passo dopo passo, garantendo soluzioni concrete, sostenibili e in linea con le esigenze aziendali.

Personalizzazione e Proporzionalità

Consapevoli che il DORA applica requisiti proporzionali alla complessità dell'organizzazione, iniziamo ogni progetto con un'analisi approfondita del contesto operativo e dei processi critici del cliente. Questo ci consente di sviluppare soluzioni su misura, evitando interventi eccessivamente gravosi per le realtà meno strutturate e garantendo al contempo la piena conformità normativa.

Coinvolgimento e Collaborazione Attiva

Riteniamo che la compliance sia efficace solo se coinvolge attivamente l'intera organizzazione. Il nostro team lavora a stretto contatto con le figure chiave del cliente, promuovendo la condivisione delle conoscenze e l'empowerment del personale interno. L'obiettivo è creare competenze stabili che permettano all'azienda di mantenere e aggiornare autonomamente le proprie procedure.

Definizione dei Referenti Interni e Collaborazione

Nell'ambito della nostra consulenza, verrà richiesto al cliente di designare internamente figure responsabili per le diverse aree aziendali coinvolte nell'attuazione delle disposizioni del DORA. Questa suddivisione di responsabilità è essenziale per garantire un'efficace gestione dei rischi ICT, una tempestiva risposta agli incidenti e la conformità ai requisiti normativi, riducendo al minimo eventuali vulnerabilità e ottimizzando il processo di adeguamento alla normativa.

Per garantire un coordinamento efficace e un'attuazione coerente delle misure previste dal DORA, il nostro Consulente NIS collaborerà attivamente con le figure interne designate dal cliente. Tale collaborazione avverrà attraverso incontri periodici strutturati, durante i quali verranno condivisi aggiornamenti sullo stato di avanzamento delle attività, eventuali criticità emerse e le azioni correttive da adottare.

La frequenza di tali incontri sarà definita in base alla complessità del progetto e alle esigenze specifiche dell'azienda, potendo variare su base settimanale, quindicinale o mensile. Nei casi in cui il livello di maturità dell'azienda in materia di gestione del rischio ICT sia ancora in fase iniziale o vi siano scadenze imminenti, si suggerirà una maggiore frequenza delle riunioni per garantire un allineamento costante e una rapida risoluzione di eventuali problematiche.

L'approccio adottato mira non solo a facilitare l'adeguamento normativo, ma anche a promuovere una cultura aziendale orientata alla sicurezza informatica, rendendo il cliente progressivamente autonomo nella gestione dei rischi digitali e nella prevenzione di minacce informatiche.

FORMALIZE: il software per la gestione integrata

Uno degli elementi distintivi della nostra consulenza è l'utilizzo del software **Formalize**, che consente una gestione efficiente e centralizzata di tutta la documentazione necessaria per la conformità al DORA. Tramite la piattaforma, il cliente potrà:

- Redigere, archiviare e aggiornare la documentazione in un ambiente digitale sicuro e facilmente accessibile.
- Monitorare in tempo reale lo stato di avanzamento delle attività tramite una dashboard intuitiva.
- Visualizzare e gestire i rischi, le vulnerabilità e le scadenze attraverso strumenti di reportistica avanzata.
- Accedere a modelli documentali standardizzati, adattabili alle specifiche esigenze dell'organizzazione.
- Ricevere notifiche automatiche sulle attività programmate, le scadenze e gli aggiornamenti normativi.

La piattaforma Formalize permette di ridurre significativamente i tempi di gestione, aumentare la trasparenza dei processi e garantire una maggiore efficienza operativa.
Nel corso della sezione successiva verranno analizzate passo dopo passo le varie fasi che sono predisposte all'interno di Formalize per effettuare un percorso di compliance completo e integrato nel rispetto di quanto previsto dal protocollo DORA.

1. Introduzione

L'introduzione al protocollo DORA (Digital Operational Resilience Act) fornisce il contesto normativo e operativo in cui le organizzazioni, in particolare quelle del settore finanziario, devono operare per garantire la propria resilienza operativa digitale. Il protocollo DORA stabilisce un quadro completo che obbliga le aziende a rafforzare la loro capacità di resistere, rispondere e riprendersi rapidamente da eventi informatici avversi, come attacchi cibernetici, guasti dei sistemi tecnologici o disastri naturali che possano compromettere l'operatività.

L'obiettivo principale di DORA è garantire che le istituzioni finanziarie e i loro fornitori di servizi ICT siano preparati a gestire e mitigare i rischi legati alla digitalizzazione. Inoltre, la normativa promuove l'integrazione delle misure di gestione del rischio ICT all'interno delle strategie aziendali globali, definendo linee guida generali per l'identificazione dei rischi, la protezione delle infrastrutture digitali e la continuità operativa. L'implementazione di tali misure diventa cruciale non solo per rispettare gli obblighi normativi, ma anche per garantire la fiducia dei clienti e la stabilità del sistema finanziario.

2. Quadro di governance

Il Quadro di governance rappresenta la struttura di controllo e supervisione necessaria per garantire la gestione efficace e continua dei rischi ICT secondo i requisiti del protocollo DORA. Questo quadro include la definizione di ruoli, responsabilità, risorse dedicate e l'impegno dell'organo di gestione nel monitorare e migliorare la resilienza operativa digitale. In base alle responsabilità verranno create differenti utenze.

2.1 Panoramica dei controlli

I controlli implementati per mitigare i rischi ICT sono fondamentali per garantire la protezione dei sistemi aziendali contro le minacce informatiche, evitando che eventi avversi possano compromettere la continuità operativa e l'integrità dei dati sensibili. L'obiettivo di questa sezione è fornire una panoramica dei controlli essenziali, suddivisi in ambiti chiave che permettano un'azione tempestiva ed efficace nella gestione del rischio. I controlli devono essere progettati per essere sia preventivi che correttivi, a seconda della fase in cui viene rilevata la minaccia o la vulnerabilità. A tal fine, l'organizzazione deve affrontare vari aspetti della sicurezza ICT, garantendo che ciascuna area di vulnerabilità sia coperta da un controllo specifico.

2.1.1 Controllo dell'Accesso ai Dati

Il controllo dell'accesso ai dati è una misura fondamentale per proteggere le informazioni sensibili e per prevenire l'accesso non autorizzato. I dati aziendali, che comprendono informazioni riservate, transazioni finanziarie, e dettagli sui clienti, devono essere adeguatamente protetti attraverso rigorosi controlli di accesso. Questi includono l'adozione di tecniche di **autenticazione multifattoriale** (MFA), che combinano diverse modalità di verifica dell'identità, e l'uso di **sistemi di gestione delle identità** per garantire che solo gli utenti autorizzati possano accedere ai dati aziendali.

Inoltre, è importante implementare politiche di accesso basate sul principio del minimo privilegio, ossia concedere agli utenti l'accesso solo alle informazioni strettamente necessarie per il loro ruolo. Un monitoraggio costante dei log di accesso e l'analisi di eventuali attività sospette è essenziale per rilevare in tempo reale accessi non autorizzati o comportamenti anomali che possano rappresentare una minaccia.

2.1.2 Gestione delle Vulnerabilità

La gestione delle vulnerabilità è un altro pilastro fondamentale per garantire la sicurezza dell'infrastruttura ICT. La protezione dai rischi derivanti da vulnerabilità nel software, hardware o nelle reti richiede un processo continuo di identificazione, valutazione e correzione delle debolezze di sicurezza. La gestione delle vulnerabilità include attività quali la scansione periodica dei sistemi alla ricerca di vulnerabilità note, l'installazione tempestiva di patch di sicurezza e l'adozione di soluzioni di hardening per ridurre le superfici di attacco.

L'implementazione di programmi di aggiornamento automatico e l'adozione di tecniche di monitoraggio proattivo dei sistemi consentono di intervenire rapidamente, riducendo il rischio che attacchi informatici possano sfruttare falle di sicurezza non corrette. Oltre alla gestione delle vulnerabilità tecniche, è cruciale anche una valutazione continua dei rischi, che possa rilevare nuove vulnerabilità emergenti o tecniche avanzate di attacco, adattando le difese aziendali di conseguenza.

2.1.3 Continuità Operativa e Risposta agli Incidenti

Infine, il controllo della continuità operativa e la risposta agli incidenti sono aspetti chiave nella protezione dei sistemi aziendali e nella gestione dei rischi ICT. Un'organizzazione deve essere in grado di continuare a operare anche in caso di attacchi informatici gravi, guasti infrastrutturali o altre emergenze. A tal fine, devono essere sviluppati **piani di continuità operativa** (BCP) e **piani di recupero di emergenza** (DRP) che definiscano le procedure da seguire per ripristinare rapidamente i servizi critici.

La risposta agli incidenti deve essere strutturata attraverso un processo ben definito che includa fasi di identificazione dell'incidente, isolamento delle minacce, analisi per comprendere la causa dell'incidente, e comunicazione trasparente con gli stakeholder. Inoltre, è essenziale effettuare simulazioni di attacco e test periodici dei piani di risposta per verificare la loro efficacia. La preparazione e la formazione del personale per gestire situazioni di emergenza sono cruciali per minimizzare i danni e ridurre i tempi di inattività.

I controlli devono essere progettati per coprire preventivamente le vulnerabilità e, se necessario, rispondere in modo efficace agli incidenti, garantendo che l'organizzazione sia pronta a far fronte a qualsiasi situazione che minacci la sua sicurezza digitale.

2.2 Identificazione dell'Organo di Gestione

L'identificazione dell'organo di gestione è un passaggio cruciale per garantire che la supervisione delle politiche ICT e dei rischi operativi digitali sia chiara e formalmente definita. L'organo di gestione, che può essere il Consiglio di Amministrazione (CdA) o un comitato dedicato alla sicurezza digitale, ha il compito di prendere decisioni strategiche sulla gestione del rischio ICT, approvare piani e politiche relative alla sicurezza informatica e monitorare le attività e le performance in questo ambito. L'efficacia del sistema di governance ICT dipende dalla sua capacità di rispondere rapidamente alle minacce emergenti e di adattarsi alle nuove normative e tecnologie.

2.2.1 Ruolo Strategico dell'Organo di Gestione

L'organo di gestione ha un ruolo strategico e decisionale fondamentale nella definizione e supervisione delle politiche aziendali relative alla sicurezza ICT. Deve essere incaricato di approvare le strategie di gestione del rischio ICT, incluse le azioni preventive e correttive, e di garantire che gli approcci adottati siano in linea con gli obiettivi generali dell'azienda. Il CdA o il comitato dedicato deve monitorare e approvare i piani di sicurezza digitale e assicurarsi che vengano adottate tutte le

misure necessarie per la protezione dei sistemi aziendali. L'organo di gestione deve inoltre rispondere alle normative vigenti, come il protocollo DORA, garantendo che l'organizzazione mantenga la resilienza digitale necessaria per operare in modo sicuro ed efficiente.

2.2.2 Comunicazione e Coinvolgimento Attivo

Un aspetto fondamentale dell'identificazione dell'organo di gestione è il suo coinvolgimento attivo nelle decisioni relative alla sicurezza ICT. Questo implica non solo l'approvazione formale delle strategie, ma anche la partecipazione diretta alla comunicazione delle attività di gestione del rischio. È essenziale che l'organo di gestione riceva report periodici e dettagliati sull'efficacia delle misure di sicurezza implementate e sui rischi emergenti, in modo da poter prendere decisioni informate e tempestive. La comunicazione tra il comitato e le altre funzioni aziendali (IT, cybersecurity, compliance) deve essere regolare e ben strutturata, assicurando che tutte le informazioni necessarie siano condivise e discusse in modo trasparente.

2.2.3 Monitoraggio Continuo e Valutazione

L'organo di gestione deve impegnarsi in un monitoraggio continuo delle attività di gestione del rischio ICT, assicurandosi che vengano raggiunti gli obiettivi strategici definiti e che le politiche di sicurezza siano efficaci e aggiornate. È necessario un processo di valutazione continua della resilienza digitale, con la revisione delle strategie e delle pratiche di sicurezza in base ai cambiamenti tecnologici, alle minacce emergenti e alle nuove normative. L'organo di gestione deve anche assicurarsi che vengano effettuati audit regolari per verificare l'efficacia delle misure di sicurezza, e che siano pronti piani di contingenza per far fronte a eventuali incidenti di sicurezza informatica.

2.3 Impegno dell'Organo di Gestione: Risorse per la Gestione del Rischio ICT

L'impegno dell'organo di gestione per allocare risorse adeguate è fondamentale per garantire una gestione efficace dei rischi ICT. Le risorse devono essere proporzionate alla complessità dell'organizzazione, considerando non solo la dimensione, ma anche il settore di operatività e il livello di esposizione ai rischi digitali. Un impegno significativo implica una selezione e allocazione strategica delle risorse, tra cui:

2.3.1 Personale Qualificato

È essenziale che l'organo di gestione assicuri la presenza di personale altamente qualificato nel campo della sicurezza informatica, della gestione dei rischi e delle tecnologie emergenti. Questo include la nomina di professionisti come il Chief Information Security Officer (CISO), team di cybersecurity, e consulenti esperti. La formazione continua e l'aggiornamento del personale sono fondamentali per mantenere un livello di competenza che risponda alle sfide tecnologiche e alle minacce in evoluzione.

2.3.2 Strumenti Tecnologici

L’azienda deve predisporre l’acquisto e la manutenzione di strumenti tecnologici avanzati per la gestione dei rischi. Questi strumenti possono comprendere software per la protezione contro malware, piattaforme di monitoraggio delle vulnerabilità, sistemi di gestione degli incidenti e delle crisi, e soluzioni di analisi predittiva per individuare minacce. È importante che l’organo di gestione si impegni anche nella valutazione periodica della performance degli strumenti, assicurando che siano aggiornati e compatibili con le tecnologie in uso.

2.3.3 Processi Strutturati per la Mitigazione dei Rischi

In aggiunta alle risorse tecnologiche e umane, è necessario che vengano definiti processi strutturati per l'identificazione, la valutazione e la mitigazione dei rischi ICT. Questi processi devono essere monitorati e continuamente migliorati, con politiche operative che permettano di affrontare situazioni di crisi e vulnerabilità in tempo utile. L’organizzazione deve assicurarsi che i processi siano adeguatamente documentati e che ci sia una comunicazione chiara e trasparente all’interno dei team.

2.4 Impegno dell’Organo di Gestione: budget

Il cliente deve predisporre un budget dedicato in modo che possa affrontare le sfide legate alla sicurezza digitale e alla protezione dei dati. Questo budget deve essere sufficiente, ben pianificato e monitorato per assicurare l’efficacia delle misure di controllo. Alcuni aspetti fondamentali da considerare includono:

2.4.1 Pianificazione del Budget

L'organo di gestione deve garantire che ci sia una pianificazione accurata del budget, tenendo conto delle priorità di sicurezza e delle risorse necessarie per affrontare i rischi informatici. La pianificazione deve essere flessibile per poter rispondere alle emergenze, come attacchi informatici imprevisti o la necessità di nuovi strumenti tecnologici. Il budget deve essere proporzionato alla dimensione e complessità delle operazioni aziendali.

2.4.2 Monitoraggio dell’Allocazione dei Fondi

Oltre a garantire la disponibilità di risorse, è fondamentale che l’organo di gestione monitori regolarmente come i fondi vengano allocati e utilizzati. L’obiettivo è garantire che tutte le spese siano giustificate e che non vi siano sprechi. L’organo di gestione deve stabilire meccanismi di verifica periodica per controllare che i fondi siano utilizzati in modo efficiente per coprire le priorità di sicurezza.

2.4.3 Copertura delle Attività Cruciali

Il budget deve essere sufficiente a coprire attività cruciali come la formazione del personale, l'acquisto di nuove tecnologie, la realizzazione di audit e test di sicurezza periodici e la partecipazione a programmi di aggiornamento continuo delle politiche di sicurezza. L'organo di gestione deve pianificare anche fondi per la gestione di incidenti imprevisti, come attacchi informatici, incidenti di violazione dei dati o interruzioni significative dei sistemi.

2.5 Impegno dell'Organo di Gestione: Ruoli, responsabilità e risorse

Una governance efficace della sicurezza ICT richiede che vengano definiti con chiarezza i ruoli e le responsabilità di tutte le persone coinvolte nella gestione dei rischi. È necessario che l'organo di gestione stabilisca delle policy operative che indichino non solo chi ha la responsabilità di cosa, ma anche le risorse disponibili per ciascun ruolo. Alcuni aspetti critici includono:

2.5.1 Definizione dei Ruoli e delle Responsabilità

Ogni membro del team coinvolto nella gestione del rischio ICT deve avere un ruolo ben definito. Le responsabilità devono essere chiaramente delineate, in modo che non ci siano ambiguità durante l'esecuzione delle attività di sicurezza. L'organo di gestione deve stabilire procedure per delegare compiti specifici e assicurarsi che ci sia un sistema di accountability, con monitoraggio e reporting trasparenti.

2.5.2 Assegnazione delle Risorse Umane e Tecniche

Le risorse necessarie per la gestione dei rischi ICT includono sia il personale che le tecnologie. L'organo di gestione deve garantire che le risorse umane e tecniche siano sufficienti e adeguate per coprire tutte le aree di rischio individuate. Questo implica la creazione di team dedicati e l'implementazione di tecnologie che possano supportare il team nell'identificazione e mitigazione dei rischi ICT.

2.5.3 Creazione di Utenze Personalizzate

Un aspetto operativo fondamentale per una gestione efficace del rischio ICT è la creazione di utenze personalizzate con permessi specifici per l'accesso alla documentazione e agli strumenti di gestione del rischio sul portale Formalize. Le utenze devono essere tracciabili e sicure, con livelli di accesso definiti in base alle responsabilità assegnate a ciascun membro del team. L'accesso ai dati e alle informazioni sensibili deve essere ristretto solo a coloro che sono coinvolti nella gestione diretta dei rischi, per garantire che le informazioni siano protette e trattate in modo sicuro.

La piattaforma Formalize è il fulcro operativo del nostro servizio. Verranno create delle utenze dedicate per l'accesso alla piattaforma Formalize con permessi di inserimento documentazione per i referenti interni coinvolti nel progetto al fine di agevolare i flussi informativi tra la Edisoft e il cliente.

Le tempistiche per il caricamento della documentazione saranno comunicate in tempo utile al fine di renderne agevole la compilazione, eventuali revisioni e il caricamento nella sezione dedicata. Grazie a questo strumento, le organizzazioni possono:

- Centralizzare e archiviare tutta la documentazione in un ambiente sicuro e conforme.
- Monitorare lo stato di avanzamento dei lavori attraverso una dashboard dedicata e di facile utilizzo.
- Ricevere notifiche automatiche per scadenze, aggiornamenti normativi e revisioni periodiche.
- Utilizzare template conformi ai requisiti DORA per velocizzare la redazione dei documenti.
- Visualizzare i rischi identificati e le azioni correttive direttamente in tempo reale.

Questa sinergia tra consulenza specializzata e tecnologia avanzata garantisce un processo più rapido, trasparente e facilmente gestibile, riducendo il carico operativo per il cliente e migliorando l'efficacia complessiva del progetto.

2.6 Impegno dell'Organo di Gestione: formazione

La formazione continua del personale è un elemento imprescindibile per garantire che tutti i livelli dell'organizzazione siano consapevoli e preparati a gestire i rischi ICT. Un programma di formazione efficace non solo sensibilizza il personale sui rischi, ma lo prepara anche ad affrontare situazioni di emergenza.

2.6.1 Programmi di Formazione Periodici

L'organo di gestione deve assicurare che vengano previsti programmi formativi periodici per tutti i dipendenti, inclusi i livelli manageriali e quelli operativi che gestiscono i sistemi critici. La formazione deve essere strutturata in base ai diversi ruoli e responsabilità, con focus su argomenti come la gestione dei rischi informatici, la protezione dei dati sensibili, e le normative di riferimento.

2.6.2 Aggiornamento Costante in Base alle Minacce

Poiché il panorama delle minacce ICT è in continua evoluzione, la formazione richiede una stretta collaborazione con esperti di settore e con i fornitori di tecnologie, per garantire che il personale sia sempre preparato a rispondere alle nuove tipologie di attacchi informatici e ai cambiamenti normativi.

2.6.3 Documentazione e Tracciamento della Formazione

Tutti i programmi di formazione devono essere documentati e tracciati in modo accurato. I responsabili della formazione devono monitorare e registrare i partecipanti ai corsi e l'efficacia della formazione stessa, per garantire che le competenze acquisite vengano applicate. I documenti formativi e le evidenze delle sessioni di formazione devono essere caricati nel portale Formalize nella sezione dedicata, per garantire la tracciabilità e l'accessibilità da parte degli organi competenti.

3. Quadro di Gestione del Rischio ICT

Il Quadro di Gestione del Rischio ICT definisce l'approccio sistematico per identificare, valutare, monitorare e mitigare i rischi legati alle tecnologie dell'informazione e della comunicazione. Questo quadro è essenziale per garantire la continuità operativa e la sicurezza dei servizi aziendali.

3.1 Strategia di Resilienza Operativa Digitale

Questa sezione definisce un piano strategico completo per garantire la continuità delle operazioni aziendali anche in caso di eventi critici, con un focus particolare sulla gestione dei rischi ICT. La strategia di resilienza operativa digitale si articola in vari piani di emergenza, ripristino e gestione delle crisi ICT, che devono essere sviluppati e implementati in modo coordinato. Questi piani includono azioni specifiche per la protezione delle infrastrutture critiche, la salvaguardia dei dati aziendali e la gestione delle comunicazioni interne ed esterne durante un incidente. La strategia deve prevedere anche test regolari, come simulazioni di attacchi o interruzioni dei sistemi, per verificarne l'efficacia e garantire che le misure di sicurezza siano sempre aggiornate rispetto alle minacce emergenti. L'obiettivo finale è assicurare che, in caso di emergenza, l'organizzazione sia in grado di ridurre al minimo l'impatto sulle operazioni e di riprendersi tempestivamente.

- Piani di emergenza e ripristino: Definizione dei processi e delle procedure da seguire in caso di eventi critici per garantire il ripristino rapido delle operazioni aziendali.
- Gestione delle crisi ICT: Strategia di risposta alle crisi digitali, con l'individuazione di team di gestione delle emergenze e comunicazione con le parti interessate.
- Test regolari e aggiornamenti: Implementazione di esercitazioni periodiche per testare l'efficacia dei piani e aggiornamenti continui delle misure di sicurezza in base ai risultati ottenuti.

3.2 Risorse e sviluppo della strategia

In questa sezione si approfondisce l'allocazione delle risorse necessarie per implementare la strategia di resilienza operativa digitale. Le risorse in questione sono di natura umana, tecnologica e finanziaria e devono essere adeguate rispetto alla dimensione e complessità dell'organizzazione. Il ruolo del personale HR diventa cruciale in quanto è necessario attrarre e formare talenti che abbiano le competenze per gestire i rischi ICT. Inoltre, il team dedicato alla resilienza operativa digitale deve essere equipaggiato con strumenti tecnologici avanzati e con un budget sufficiente a coprire le attività previste.

L'allocazione delle risorse non si limita alla sola fase di implementazione ma deve essere mantenuta costante nel tempo, con un monitoraggio continuo per garantire che le risorse siano sempre adeguate a fronte delle evoluzioni del contesto normativo e tecnologico.

- Allocazione delle risorse umane: Identificazione e formazione di un team competente che gestisca la resilienza operativa digitale, con il supporto delle risorse HR.

- **Tecnologia e infrastruttura**: Investimento in soluzioni tecnologiche avanzate per la protezione dei sistemi informatici e l'adozione di strumenti adeguati per la gestione dei rischi.
- **Allocazione del budget**: Previsione di un budget dedicato alla resilienza operativa digitale, da utilizzare per la formazione, l'acquisto di nuove tecnologie e l'aggiornamento continuo delle risorse.

3.3 Ruoli di gestione del Rischio

Definire i ruoli e le responsabilità all'interno dell'organizzazione è un passo fondamentale per la gestione efficace del rischio ICT. Ogni membro dell'organizzazione deve essere consapevole del proprio ruolo nella protezione dei sistemi informatici e della continuità operativa. In particolare, è essenziale stabilire un chiaro sistema di deleghe e supervisione che assicuri un flusso di informazioni efficiente e tempestivo. Ogni funzione critica dell'organizzazione deve essere coperta da figure specifiche che siano in grado di prendere decisioni rapide e informate in caso di emergenza. La gestione del rischio ICT, infatti, non deve essere vista come una responsabilità centralizzata, ma come un impegno condiviso tra vari livelli organizzativi, con una catena di comando ben strutturata e un monitoraggio continuo delle attività.

- **Assegnazione delle responsabilità**: Identificazione dei responsabili per la gestione di specifici rischi ICT, come la protezione dei dati e la gestione delle crisi.
- **Deleghe e supervisione**: Creazione di un sistema di deleghe chiaro e trasparente, con un focus sulle figure manageriali che devono garantire la continuità operativa.
- **Flusso di informazioni**: Implementazione di un sistema che garantisca la comunicazione tempestiva e corretta delle informazioni tra i vari livelli dell'organizzazione.

3.4 Revisione dell'Audit Interno

La revisione dell'audit interno rappresenta una fase cruciale per valutare l'efficacia delle misure di gestione del rischio ICT. Un audit regolare permette di identificare eventuali non conformità o debolezze nei processi aziendali e di proporre azioni correttive per migliorare la resilienza operativa digitale. L'audit dovrebbe essere condotto periodicamente, con un focus sulle aree più critiche, e includere sia verifiche tecniche (ad esempio, vulnerabilità nei sistemi informatici) sia controlli sui processi aziendali. Le azioni correttive dovrebbero essere implementate rapidamente e monitorate nel tempo per garantire che l'organizzazione rimanga sempre conforme agli standard e alle normative di riferimento, evitando sanzioni o errori nelle documentazioni richieste.

- **Verifiche periodiche**: Pianificazione e realizzazione di audit periodici per valutare l'efficacia delle misure di gestione del rischio ICT.
- **Identificazione delle non conformità**: Individuazione delle aree in cui l'organizzazione non rispetta i requisiti normativi o presenta vulnerabilità.
- **Azioni correttive e follow-up**: Implementazione di misure correttive per risolvere le non conformità identificate e monitoraggio continuo dell'efficacia delle soluzioni adottate.

3.5 Valutazione della compliance della Gestione del Rischio ICT

Questa sezione è dedicata alla verifica della conformità delle pratiche di gestione del rischio ICT rispetto alle normative vigenti, con particolare attenzione al protocollo DORA. Una gestione del rischio ICT conforme alle normative è fondamentale per evitare problematiche legali o operative. Il processo di valutazione della compliance include la verifica continua delle politiche e delle procedure interne, assicurando che siano allineate con gli standard previsti dal protocollo DORA. In caso di necessità, i nostri consulenti forniranno supporto ai responsabili interni dell'organizzazione per garantire l'autonomia nella gestione della compliance. Verranno inoltre messi a disposizione i testi di legge aggiornati per permettere a tutti i dipendenti di operare nel pieno rispetto delle normative.

- Verifica delle politiche interne: Monitoraggio delle politiche aziendali per garantirne la conformità alle normative DORA.
- Supporto ai responsabili: Fornitura di supporto pratico ai responsabili interni per risolvere eventuali criticità nella gestione del rischio ICT.
- Condivisione della normativa: Fornitura di testi di legge e aggiornamenti continui per garantire che tutto il personale sia sempre informato sugli obblighi di compliance.

4. Fonti di conoscenza sulla Gestione del Rischio ICT

Le fonti di conoscenza sono fondamentali per mantenere aggiornate le strategie e le pratiche di gestione del rischio ICT. Esse forniscono informazioni essenziali per migliorare continuamente i processi di resilienza operativa aziendale.

4.1 Fonti di conoscenza: Miglioramento continuo

Il miglioramento continuo è un processo essenziale per mantenere e rafforzare la sicurezza aziendale e la gestione dei rischi nel tempo. In un mondo in rapida evoluzione, dove le minacce e i rischi cambiano costantemente, è fondamentale che le aziende utilizzino fonti di conoscenza per adattarsi alle nuove sfide e perfezionare le misure di protezione. Questo processo non solo migliora la resilienza dell'organizzazione, ma assicura anche che le decisioni strategiche siano basate su dati accurati, aggiornati e pertinenti. Il miglioramento continuo si fonda sull'analisi dei dati, la raccolta di feedback, e l'apprendimento dalle esperienze passate, consentendo di evolvere le politiche e le pratiche aziendali in modo dinamico.

4.1.1 Utilizzo dei Dati per il Miglioramento Continuo

I dati raccolti attraverso diverse fonti (come log di sistema, report di sicurezza, monitoraggio delle attività aziendali e feedback dei dipendenti) rappresentano un patrimonio fondamentale per il miglioramento continuo. Analizzando i dati, è possibile identificare pattern e tendenze che potrebbero passare inosservati in un'analisi superficiale. I dati, infatti, permettono di:

- Valutare l'efficacia delle misure di sicurezza: Monitorando costantemente gli incidenti di sicurezza e le risposte ad essi, si può verificare se le misure di sicurezza esistenti sono sufficienti o necessitano di modifiche.
- Identificare anomalie e vulnerabilità: L'analisi dei dati può mettere in luce potenziali vulnerabilità che non erano state precedentemente identificate, come configurazioni errate o accessi non autorizzati.
- Monitorare e migliorare la risposta agli incidenti: I dati relativi agli incidenti di sicurezza, come i tempi di risposta, la gestione degli impatti e la comunicazione interna, forniscono indicazioni su come migliorare la reattività dell'organizzazione a situazioni critiche.

Un aspetto fondamentale dell'utilizzo dei dati per il miglioramento continuo è la creazione di un ciclo di feedback, dove i risultati ottenuti dai dati vengono utilizzati per perfezionare ulteriormente le politiche e le procedure aziendali.

4.1.2 L'Importanza dei Report per il Miglioramento Continuo

I report sono strumenti cruciali per il miglioramento continuo, poiché forniscono una documentazione chiara e dettagliata sull'andamento delle operazioni aziendali, le performance delle misure di sicurezza, e gli sviluppi relativi ai rischi.

Alcuni dei report fondamentali includono:

- Report di incidenti e risposte: Ogni incidente di sicurezza o rischio significativo deve essere documentato, insieme alle azioni intraprese per risolverlo. L'analisi di questi report aiuta a identificare le aree di miglioramento nella gestione delle crisi.
- Report sulle minacce emergenti: Questi report offrono una panoramica sulle minacce in evoluzione, basandosi su dati globali, tendenze di settore e analisi di incidenti recenti. Questi documenti sono fondamentali per prevedere e prepararsi a minacce future.
- Report di audit di sicurezza: Le verifiche periodiche e gli audit di sicurezza offrono un'analisi oggettiva dei sistemi e delle politiche di sicurezza aziendale, permettendo di identificare lacune e suggerire miglioramenti.

4.1.3 Raccolta e Analisi del Feedback

Il feedback è una risorsa estremamente preziosa per il miglioramento continuo. Non solo aiuta a identificare le aree di debolezza nelle operazioni aziendali, ma fornisce anche spunti su come rafforzare i processi di gestione dei rischi. Le fonti di feedback possono essere suddivise in:

- Feedback dai dipendenti: I dipendenti sono in prima linea nell'interagire con i processi aziendali e possono fornire osservazioni dirette sulle debolezze operative o sulle difficoltà nel rispettare le misure di sicurezza. I loro suggerimenti sono cruciali per migliorare le pratiche quotidiane e ottimizzare i protocolli di sicurezza.
- Feedback dai clienti: Le interruzioni dei servizi, i problemi di sicurezza o le preoccupazioni relative alla privacy possono emergere attraverso il feedback dei clienti. Comprendere le loro esperienze e le loro esigenze aiuta l'azienda a modificare le sue politiche e a rispondere meglio alle aspettative del mercato.
- Feedback dai fornitori e partner: I fornitori di tecnologie e soluzioni possono contribuire con feedback preziosi sulle vulnerabilità emergenti e sulle best practices per proteggere le infrastrutture critiche.

4.1.4 Analisi delle Tendenze e delle Minacce Emergenti

L'analisi delle tendenze è una componente essenziale del miglioramento continuo, in quanto consente all'azienda di anticipare potenziali rischi e di adottare misure preventive. Le minacce evolvono costantemente, e l'azienda deve essere pronta a reagire a nuovi attacchi, cambiamenti normativi, o sviluppi tecnologici. Alcuni aspetti importanti da considerare includono:

- Minacce informatiche in evoluzione: Gli attacchi informatici, come il phishing, il ransomware o gli attacchi DDoS, sono in continua evoluzione. Le aziende devono rimanere aggiornate su nuovi metodi di attacco e adottare soluzioni avanzate per contrastarli.
- Rischi normativi: Cambiamenti nelle normative di sicurezza, privacy e compliance, come il GDPR o la direttiva NIS2, possono comportare nuovi rischi che richiedono l'adeguamento delle politiche aziendali.
- Sostenibilità e cambiamenti climatici: L'aumento dei disastri naturali legati al cambiamento climatico rappresenta una nuova minaccia per la continuità operativa, che le aziende devono tenere in considerazione nella gestione dei rischi.

4.1.5 Lezioni Apprese dagli Incidenti Passati

Un aspetto cruciale del miglioramento continuo è l'apprendimento dalle esperienze passate. Ogni incidente di sicurezza o crisi aziendale offre lezioni che possono essere utilizzate per perfezionare le procedure esistenti e ridurre la probabilità di futuri fallimenti. Le lezioni apprese possono riguardare:

- Carenze nei piani di risposta: Durante un incidente, potrebbero emergere carenze nei piani di emergenza che necessitano di essere migliorati.
- Mancato aggiornamento delle tecnologie: Un incidente potrebbe rivelare che le tecnologie di protezione non sono adeguate o non sono state aggiornate.
- Problemi di comunicazione interna ed esterna: Un altro insegnamento può derivare da difficoltà nel coordinamento delle risposte tra i vari team aziendali o nella comunicazione con i clienti e i partner.

Queste lezioni, una volta analizzate, devono essere integrate nei processi aziendali per evitare che vengano ripetuti gli stessi errori.

4.1.6 Utilizzo dei Questionari per la Valutazione Oggettiva

Per raccogliere dati e feedback in modo strutturato e integrato, le aziende possono utilizzare questionari mirati. Questi strumenti aiutano a valutare in modo oggettivo e sistematico le tendenze emergenti, i rischi percepiti e le potenziali minacce, così come la percezione della sicurezza all'interno dell'organizzazione. I questionari possono essere indirizzati a diverse categorie di stakeholder, come dipendenti, clienti, partner, e responsabili della sicurezza, e devono coprire aree specifiche come:

- Valutazione della sicurezza informatica: Domande relative alla protezione dei dati, alle minacce informatiche recenti e alla preparazione dell'azienda per fronteggiare nuovi attacchi.
- Valutazione dei processi operativi: Domande su come i processi aziendali si stanno adattando alle nuove minacce e se ci sono aree vulnerabili da migliorare.
- Percezione della gestione dei rischi: Domande per valutare come le politiche di gestione dei rischi vengono recepite dai dipendenti e quanto efficaci sono percepite.

Il miglioramento continuo non è un processo statico, ma un ciclo dinamico che richiede l'utilizzo costante di dati, feedback, e analisi delle tendenze emergenti. L'adozione di questionari strutturati, la raccolta e l'analisi delle lezioni apprese da incidenti passati, e la valutazione delle minacce emergenti sono pratiche che devono essere integrate in una strategia complessiva di gestione dei rischi. In questo modo, l'azienda può migliorare costantemente la sua resilienza e prepararsi adeguatamente per affrontare le sfide future.

4.2 Fonti di conoscenza: Verifica e risanamento

Il processo di verifica e risanamento rappresenta una componente critica nella gestione della sicurezza e dei rischi aziendali. Dopo che una vulnerabilità o un incidente viene rilevato, è essenziale avviare una serie di attività di controllo e intervento correttivo per garantire che il problema venga risolto efficacemente, le cause principali vengano identificate e che vengano implementate misure preventive per evitare il ripetersi di eventi simili in futuro. Il risanamento non riguarda solo la risoluzione immediata dei problemi, ma implica un'analisi approfondita e un intervento strutturato che punti a migliorare il sistema e a rendere l'organizzazione più resiliente contro rischi futuri.

4.2.1 Controllo e Monitoraggio delle Vulnerabilità

Il controllo delle vulnerabilità è un processo continuo che implica la ricerca attiva di punti deboli nei sistemi, nei processi e nelle pratiche aziendali. La verifica viene realizzata attraverso una combinazione di strumenti automatici, analisi manuale e audit periodici, e ha lo scopo di rilevare potenziali minacce che potrebbero compromettere la sicurezza aziendale. Queste attività comprendono:

- Scansione delle vulnerabilità: L'uso di software specializzati per identificare vulnerabilità nei sistemi IT, nei server, nelle reti e nei dispositivi aziendali. Le scansioni devono essere regolari e puntuali per rilevare anche minacce emergenti.
- Penetration testing (Test di penetrazione): Simulazione di attacchi informatici mirati a verificare l'efficacia delle difese aziendali. Questo processo aiuta a scoprire le debolezze nei sistemi prima che possano essere sfruttate da attori malintenzionati.
- Audit della sicurezza: Revisione completa dei sistemi informatici, delle politiche e delle pratiche di sicurezza aziendali. Gli audit possono essere interni o esterni e dovrebbero essere condotti periodicamente per garantire la conformità e l'efficacia delle misure di protezione.

4.2.2 Analisi delle Cause Principali degli Incidenti (RCA)

Quando si verifica un incidente di sicurezza o si identificano vulnerabilità, l'analisi delle cause principali (Root Cause Analysis, RCA) è una parte fondamentale del processo di risanamento. Questo processo prevede l'esame approfondito di tutte le circostanze che hanno portato all'incidente per identificare non solo il problema immediato ma anche le cause sottostanti che ne hanno permesso la manifestazione. La RCA include:

- Esame dei fattori tecnici: Identificazione di problemi legati alla tecnologia, come software obsoleti, configurazioni errate o mancanza di aggiornamenti critici.
- Esame dei fattori umani: Considerazione degli errori umani che potrebbero aver contribuito all'incidente, come la mancanza di formazione, la negligenza o la gestione inadeguata delle password.
- Esame dei processi aziendali: Verifica della robustezza dei processi aziendali, come la gestione dei dati sensibili, la risposta agli incidenti e la gestione delle risorse. La mancata applicazione di procedure adeguate può essere una delle cause principali.

L’obiettivo dell’analisi delle cause principali è di arrivare a una comprensione completa dell’incidente e di come si può impedire che simili problematiche si ripetano in futuro.

4.2.3 Implementazione delle Misure Correttive

Una volta che le cause principali sono state identificate, è necessario agire con misure correttive mirate. Queste azioni correttive dovrebbero affrontare direttamente le debolezze emerse e implementare soluzioni che migliorino la sicurezza, l'affidabilità e la resilienza dei sistemi aziendali. Alcuni esempi di misure correttive includono:

- Aggiornamento e patching dei sistemi: Implementazione di aggiornamenti e patch di sicurezza per correggere vulnerabilità note. Questo è particolarmente cruciale per i sistemi informatici e le applicazioni aziendali che, se non mantenuti aggiornati, possono essere bersaglio di attacchi.
- Rafforzamento delle politiche di sicurezza: Rivedere e migliorare le politiche aziendali relative alla sicurezza, come le linee guida sull’uso delle password, le procedure di accesso ai sistemi e la protezione dei dati.
- Revisione della formazione del personale: Se gli errori umani sono stati una causa significativa dell’incidente, è necessario implementare programmi di formazione e sensibilizzazione sulla sicurezza, affinché tutti i dipendenti siano consapevoli dei rischi e dei comportamenti sicuri.
- Automatizzazione delle risposte agli incidenti: Implementazione di soluzioni automatizzate per rilevare e rispondere rapidamente agli incidenti di sicurezza. Ciò riduce il tempo di reazione e limita i danni in caso di nuove minacce.

L’efficacia delle misure correttive deve essere continuamente monitorata, e gli impatti di queste azioni devono essere valutati per garantire che il rischio sia effettivamente mitigato.

4.2.4 Prevenzione del Ripetersi di Eventi Simili

Il vero scopo del risanamento non è solo risolvere un incidente, ma impedire che si verifichi nuovamente in futuro. Per fare ciò, è necessario stabilire un ciclo di miglioramento continuo, dove ogni incidente fornisce un'opportunità per rafforzare le difese aziendali. Alcune azioni preventive includono:

- Modifica dei processi aziendali: Quando un incidente è legato a una lacuna nei processi aziendali, è necessario apportare modifiche a livello di procedure operative per evitare che errori simili possano ripetersi.
- Miglioramento delle soluzioni di monitoraggio: Implementazione di sistemi avanzati di monitoraggio e analisi, che siano in grado di rilevare e segnalare attività sospette prima che possano evolvere in un incidente grave.
- Pianificazione della resilienza a lungo termine: Costruire una cultura della sicurezza che vada oltre la risposta agli incidenti, includendo la pianificazione della resilienza a lungo termine. Ciò significa sviluppare piani di disaster recovery, strategie di backup e garantire la continuità operativa in caso di eventi imprevisti.

Le azioni preventive devono essere documentate e integrate in un piano di gestione dei rischi globale, che viene continuamente aggiornato e migliorato sulla base delle nuove informazioni e delle lezioni apprese.

4.2.5 Monitoraggio e Verifica dell'Efficacia delle Misure Correttive

Dopo l'attuazione delle misure correttive, è fondamentale monitorare costantemente l'efficacia di tali misure per verificare se gli obiettivi di sicurezza siano stati effettivamente raggiunti. Il monitoraggio deve comprendere:

- Test periodici di sicurezza: Verifiche regolari attraverso penetration testing e scansioni di vulnerabilità per garantire che le misure implementate siano sufficienti a proteggere contro i rischi identificati.
- Revisione dei report di incidenti: Monitoraggio dei report sugli incidenti futuri per accertarsi che la frequenza e la gravità degli eventi siano diminuiti e che non si ripetano gli stessi problemi.
- Valutazione continua dei processi aziendali: Analisi periodica delle procedure operative per assicurarsi che le modifiche siano state correttamente implementate e che siano ancora in linea con le migliori pratiche del settore.

Un approccio iterativo e continuo di monitoraggio e verifica garantisce che le misure correttive non siano solo una risposta immediata a un singolo evento, ma una parte integrante di un sistema di gestione dei rischi che evolve e si adatta nel tempo.

Il processo di verifica e risanamento è cruciale per mantenere la sicurezza aziendale nel tempo. Dopo la rilevazione di vulnerabilità o incidenti, le attività di controllo e le azioni correttive devono essere eseguite con l'obiettivo di non solo risolvere i problemi immediati, ma anche di identificare le cause principali e prevenire il ripetersi degli eventi. L'analisi approfondita, la correzione delle vulnerabilità e l'adozione di misure preventive sono essenziali per costruire un sistema di gestione dei rischi più forte e resiliente, che protegga l'azienda nel lungo periodo.

5. Identificazione delle fonti di rischio

Questa sezione è dedicata all'identificazione sistematica delle potenziali fonti di rischio che possono compromettere la sicurezza e la continuità delle operazioni ICT. Con il software Formalize, sarà possibile verificare e analizzare le diverse fonti di rischio ICT attraverso una **Risk Probability-Impact Matrix**. Questo grafico consente di valutare visivamente i rischi associati a vari fattori, classificandoli in base alla loro probabilità di accadimento e al potenziale impatto. Utilizzando la matrice, i team di gestione della sicurezza potranno identificare facilmente i rischi critici, con colori che evidenziano le aree a maggiore priorità (rosso per alto rischio, arancione per moderato e verde per basso rischio), facilitando così l'adozione di misure preventive e correttive in modo tempestivo e mirato.

5.1 Identificazione delle operazioni e degli asset

L'identificazione delle operazioni aziendali e degli asset critici è un passaggio fondamentale per garantire una gestione efficace dei rischi e una solida strategia di continuità operativa. Questo processo implica la mappatura dettagliata delle operazioni vitali per il funzionamento dell'azienda, degli asset che le supportano, e delle risorse necessarie per la realizzazione di tali operazioni. La mappatura deve includere una valutazione dei sistemi informatici, delle infrastrutture fisiche e dei dati sensibili, considerando come ognuno di questi asset influisca sulla resilienza complessiva dell'azienda. Solo attraverso una comprensione precisa di questi elementi, un'azienda può stabilire le giuste priorità nella gestione dei rischi e pianificare soluzioni efficaci per proteggerli.

5.1.1 Mappatura delle Operazioni Aziendali Critiche

Ogni azienda svolge una serie di operazioni quotidiane che sono essenziali per il raggiungimento dei propri obiettivi e per garantire il funzionamento regolare. Queste operazioni devono essere individuate e classificate in base alla loro importanza strategica. Alcuni esempi di operazioni critiche includono:

- **Produzione e distribuzione**: Ogni operazione legata alla produzione dei beni o servizi offerti dall'azienda, inclusi i processi di approvvigionamento, gestione della supply chain, e distribuzione.
- **Assistenza clienti**: Servizi di supporto che mantengono la relazione con il cliente, dalla gestione delle richieste di assistenza alla manutenzione del servizio post-vendita.
- **Sistemi di pagamento e transazioni finanziarie**: Operazioni finanziarie interne come la gestione della liquidità, pagamenti e gestione dei conti aziendali, che sono fondamentali per il corretto funzionamento finanziario dell'azienda.
- **Gestione delle risorse umane**: Dalla selezione e formazione del personale alla gestione delle buste paga e dei benefit, fino alla gestione delle crisi interne che potrebbero influire sul benessere organizzativo.
- **Compliance legale e gestione dei contratti**: La gestione di tutte le funzioni legate al rispetto delle normative, della privacy e dei contratti con i fornitori, partner e clienti.

5.1.2 Identificazione degli Asset Critici

Gli asset aziendali sono risorse fondamentali per il funzionamento delle operazioni aziendali e possono essere suddivisi in diverse categorie. La loro protezione è essenziale per garantire la continuità operativa in caso di eventi imprevisti. Gli asset critici più comuni includono:

- **Sistemi informatici e software**: I sistemi IT aziendali che permettono la gestione delle informazioni, la comunicazione interna e l'elaborazione dei dati, come i server, le applicazioni software, i database e le piattaforme cloud.
- **Infrastrutture fisiche**: Gli impianti fisici come gli uffici, i magazzini, le attrezzature di produzione, le reti di distribuzione energetica e altri beni tangibili necessari per il funzionamento operativo dell'azienda.
- **Dati sensibili e informazioni aziendali**: Dati relativi ai clienti, ai dipendenti, alle operazioni aziendali o a proprietà intellettuali che necessitano di protezione per evitare danni economici e reputazionali. Questi dati possono includere informazioni finanziarie, strategiche, contrattuali o di ricerca e sviluppo.
- **Rete di comunicazione**: La rete di telecomunicazioni, comprese le connessioni Internet, i sistemi di telefonia e i canali di comunicazione interna, che consentono la gestione quotidiana e la comunicazione aziendale.
- **Fornitori e partner strategici**: Le risorse esterne come fornitori di materie prime, software, servizi cloud, consulenti, e partner commerciali che supportano il funzionamento aziendale.

5.1.3 Analisi delle Interdipendenze tra Operazioni e Asset

Una volta identificati gli asset critici, è essenziale mappare le interdipendenze tra operazioni e asset per comprendere come ciascun elemento influisce sull'altro e come un malfunzionamento di un asset possa avere impatti a cascata su altre funzioni aziendali. Ad esempio, un'interruzione del sistema informatico aziendale potrebbe bloccare non solo la produzione, ma anche l'assistenza clienti, la gestione finanziaria e la comunicazione con i fornitori.

5.1.4 Prioritizzazione dei Rischi

La mappatura degli asset critici e delle operazioni aziendali permette di stabilire le priorità nella gestione dei rischi. È fondamentale, infatti, che l'azienda si concentri prima sugli asset che sono più vulnerabili o che, se compromessi, potrebbero causare danni più gravi. La priorizzazione dei rischi può essere effettuata attraverso l'utilizzo di diversi strumenti e metodologie, tra cui:

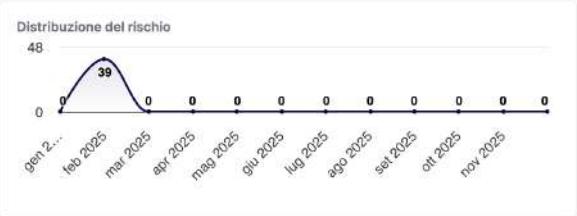
- **Analisi di impatto aziendale (BIA)**: Un processo che aiuta a identificare le funzioni aziendali più critiche e le risorse necessarie per il loro supporto, determinando quali sono le aree che, se compromesse, potrebbero comportare il maggiore impatto economico o operativo.
- **Valutazione del rischio**: Una valutazione sistematica di ogni rischio, basata sulla probabilità di accadimento e sull'impatto che l'interruzione di un asset o di un'operazione critica potrebbe avere sull'azienda. Ad esempio, un attacco informatico che comprometta i dati sensibili potrebbe avere un impatto maggiore rispetto a una perdita temporanea di connessione a Internet.

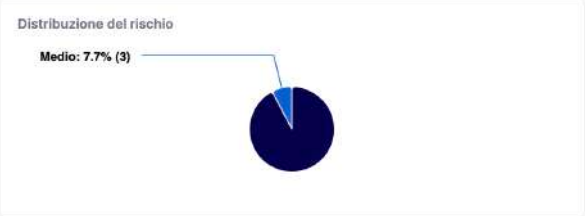
5.1.5 Utilizzo di Grafici per la Gestione dei Rischi

I grafici e le visualizzazioni possono essere strumenti molto utili per rappresentare le informazioni relative agli asset critici e alle operazioni aziendali, facilitando l'analisi e la comunicazione. Tra i principali strumenti grafici utilizzati ci sono:

- **Matrice di rischio**: Un grafico che incrocia la probabilità di un evento con l'impatto che questo avrebbe sull'azienda, aiutando a visualizzare quali rischi richiedono una gestione prioritaria.
- **Diagramma di flusso delle operazioni**: Un diagramma che illustra i flussi di lavoro e le interdipendenze tra le operazioni aziendali e gli asset che le supportano. Questo strumento permette di comprendere le relazioni critiche tra vari processi e risorse.
- **Heat-map dei rischi**: Una mappa a colori che rappresenta visivamente la gravità dei rischi in base alla loro probabilità e impatto. Questo tipo di grafico è utile per evidenziare le aree più vulnerabili e le priorità da affrontare.

La mappatura delle operazioni aziendali e degli asset critici è il primo passo fondamentale per sviluppare un piano di gestione dei rischi efficace. Identificando e priorizzando le risorse più vitali per l'azienda, è possibile attuare strategie di protezione adeguate che garantiscano la continuità operativa in caso di crisi. L'analisi delle interdipendenze e l'utilizzo di strumenti grafici permettono di visualizzare chiaramente la rete di risorse critiche e di intervenire in modo mirato per ridurre al minimo i rischi.





5.2 Identificazione delle operazioni e degli asset: funzioni aziendali

La continuità operativa è fondamentale per garantire che un'azienda possa mantenere le sue funzioni principali anche di fronte a eventi imprevisti, come attacchi informatici, disastri naturali o guasti tecnici. Per fare ciò, è essenziale identificare e proteggere le funzioni aziendali critiche, che sono le fondamenta su cui si costruisce l'efficienza operativa e la capacità di generare valore. Un'analisi dei processi aziendali chiave e delle loro interdipendenze è cruciale per individuare le aree vulnerabili e attuare strategie di protezione adeguate.

5.2.1 Identificazione delle Funzioni Aziendali Essenziali

Le funzioni aziendali essenziali sono quelle attività senza le quali l'azienda non può operare correttamente o rischia di subire gravi danni. Queste includono:

1. **Gestione delle operazioni**: Tutte le attività che permettono la produzione e la distribuzione di beni o servizi, inclusi i processi di approvvigionamento, produzione, logistica e distribuzione.
2. **Gestione delle risorse umane**: La gestione dei dipendenti, dalla selezione, formazione, retribuzione e sviluppo del personale, fino alla gestione di situazioni critiche come licenziamenti e malattia.
3. **Funzioni di supporto IT**: I sistemi informativi e le infrastrutture tecnologiche, come server, reti e database, sono essenziali per garantire la comunicazione interna ed esterna e la gestione dei dati.
4. **Gestione delle finanze**: Le funzioni che si occupano della gestione dei flussi di cassa, contabilità, finanza e reportistica, che sono fondamentali per la stabilità economica dell'azienda.
5. **Servizio clienti e supporto**: La gestione delle richieste e dei problemi dei clienti è cruciale per mantenere la soddisfazione del cliente e garantire la fidelizzazione.
6. **Compliance e sicurezza legale**: Le funzioni che assicurano che l'azienda rispetti le normative locali e internazionali in materia di sicurezza, privacy e responsabilità sociale.

5.2.2 Analisi dei Processi Chiave e delle Interdipendenze

Una volta identificate le funzioni aziendali critiche, è necessario eseguire un'analisi approfondita dei processi chiave e delle loro interdipendenze per valutare come un'interruzione in una funzione possa impattare le altre aree dell'azienda. Questo processo include:

1. **Mappatura dei processi**: Ogni funzione deve essere mappata e analizzata per identificare i flussi di lavoro, le risorse utilizzate e gli output generati. Ad esempio, un'interruzione del sistema informatico può bloccare l'accesso ai dati finanziari, impedendo l'approvazione dei pagamenti e la gestione del bilancio.
2. **Valutazione delle vulnerabilità**: Ogni processo aziendale deve essere esaminato per individuare eventuali vulnerabilità. Queste possono riguardare dipendenze critiche da risorse esterne, come fornitori di servizi cloud o logistica di terze parti, che, se non protette adeguatamente, possono creare interruzioni nel flusso delle attività.

3. Analisi delle interdipendenze: I vari processi aziendali sono strettamente interconnessi. L'interruzione di un processo, come la gestione delle risorse umane, può avere un impatto diretto sulla capacità di produzione o sulla qualità del servizio clienti. Ad esempio, un disguido nella gestione delle paghe potrebbe causare disordini tra i dipendenti, impattando negativamente sulla produttività.
4. Gestione del rischio: Una volta identificate le vulnerabilità e le interdipendenze, l'azienda deve sviluppare un piano di gestione del rischio. Questo include la definizione di misure preventive (come backup dei dati e protezione delle infrastrutture IT), piani di recupero in caso di guasto (disaster recovery) e strategie di continuità operativa (business continuity). Tali piani devono essere regolarmente testati e aggiornati per adattarsi a nuove minacce o cambiamenti nel contesto aziendale.

5.2.3 Implementazione delle Misure di Protezione

A seguito dell'analisi, le aziende devono implementare misure concrete per proteggere le funzioni critiche e garantire la loro continuità. Le principali misure includono:

1. Piani di continuità operativa (BCP): Questi piani stabiliscono come riprendere rapidamente le operazioni aziendali dopo un'interruzione. Devono coprire tutti gli aspetti, dalle risorse umane alla gestione dei sistemi IT.
2. Sistemi di backup e recupero dati: Essenziali per garantire che le informazioni aziendali siano protette e recuperabili in caso di guasti ai sistemi principali. È fondamentale stabilire procedure per la creazione regolare di copie di sicurezza.
3. Protezione della sicurezza informatica: L'implementazione di sistemi di protezione come firewall, antivirus, e crittografia è essenziale per difendere i dati aziendali e la rete da attacchi esterni.
4. Formazione e sensibilizzazione del personale: Un aspetto spesso trascurato ma cruciale è la preparazione del personale. I dipendenti devono essere addestrati a riconoscere e gestire le situazioni di rischio, come attacchi di phishing o interruzioni di servizio.

Proteggere le funzioni aziendali essenziali è un compito fondamentale per garantire la continuità operativa. L'analisi approfondita dei processi chiave e delle loro interdipendenze consente di identificare le vulnerabilità e di sviluppare piani di protezione e recupero efficaci. Le aziende devono non solo proteggere le risorse critiche, ma anche garantire che tutti i processi siano resilienti e in grado di rispondere rapidamente a qualsiasi tipo di emergenza.

5.3 Identificazione delle operazioni e degli asset: Asset informativi e ICT

L'identificazione degli asset informativi e ICT è una componente cruciale nella gestione dei rischi aziendali, poiché le risorse tecnologiche e informative sono fondamentali per il corretto funzionamento e la competitività di un'organizzazione. Una corretta mappatura e valutazione di questi asset consente di comprendere quali siano i sistemi e le risorse critiche, al fine di proteggerli adeguatamente contro le minacce informatiche. Questo processo non si limita solo a identificare i singoli componenti tecnologici, ma comprende anche una valutazione del loro impatto sul business e della loro vulnerabilità rispetto a potenziali attacchi o eventi di natura informatica.

5.3.1 Mappatura degli Asset Informativi e ICT

La mappatura degli asset ICT implica un'analisi dettagliata delle risorse tecnologiche che compongono l'infrastruttura aziendale. Questi asset sono essenziali per l'operatività quotidiana e la gestione delle informazioni. Gli asset identificati vengono classificati in base alla loro rilevanza e criticità per il business, comprendendo:

- Hardware: Include server, dispositivi di rete (router, switch, firewall), workstation, dispositivi mobili aziendali (laptop, tablet, smartphone) e dispositivi IoT (Internet of Things) che connettono l'infrastruttura fisica dell'organizzazione alla rete. Ogni dispositivo hardware deve essere valutato in termini di utilizzo aziendale e potenziale impatto se compromesso.
- Software: Consiste nei sistemi operativi, applicazioni aziendali, software di produttività, software di sicurezza, database e applicazioni cloud. Ogni applicazione o programma deve essere valutato per la sua capacità di gestire dati sensibili, di supportare operazioni critiche e di interfacciarsi con altre tecnologie aziendali.
- Reti: Le reti aziendali, incluse LAN (Local Area Network), MAN (Metropolitan Area Network), VPN (Virtual Private Network), Wi-Fi e altre connessioni che consentono la comunicazione e il trasferimento di dati tra le risorse aziendali. La sicurezza della rete è vitale per prevenire attacchi esterni, come gli attacchi DDoS (Distributed Denial of Service) o le intrusioni non autorizzate.
- Basi Dati: Le banche dati contenenti informazioni vitali per l'organizzazione, come dati finanziari, dati dei clienti, inventari, e altri dati sensibili. L'integrità e la sicurezza di queste informazioni sono cruciali per evitare il furto, la perdita o la corruzione dei dati.

5.3.2 Valutazione dell'Importanza e della Criticità degli Asset

Una volta identificati gli asset informativi e ICT, è necessario valutarne l'importanza per le operazioni aziendali. Ogni asset ha un valore diverso a seconda di come influisce sulle attività e sugli obiettivi strategici dell'organizzazione. La valutazione di criticità può essere effettuata attraverso i seguenti criteri:

- Impatto sul business: Determinare quanto dipende l'organizzazione da ciascun asset per mantenere la continuità operativa. Per esempio, un sistema ERP che gestisce la produzione e la logistica di un'azienda è cruciale rispetto a una semplice applicazione di messaggistica interna.

- Dipendenza dalle tecnologie: Alcune attività aziendali possono dipendere in modo critico da specifici strumenti tecnologici. Un'interruzione in un sistema di gestione dei dati o un malfunzionamento della rete potrebbe paralizzare l'attività dell'intera organizzazione.
- Accesso a dati sensibili: Gli asset che contengono o gestiscono dati sensibili, come le informazioni sui clienti, i dati finanziari e i segreti aziendali, sono considerati di alta criticità. La protezione di questi dati è essenziale per evitare il furto di informazioni o l'esposizione a rischi legali e reputazionali.
- Interconnessione tra sistemi: La valutazione dell'interconnessione tra diversi sistemi e asset è fondamentale. Un asset che interagisce con molteplici altri asset potrebbe essere più vulnerabile a potenziali falle di sicurezza, rappresentando un punto di attacco strategico per un cybercriminale.

5.3.3 Analisi della Vulnerabilità degli Asset

Una volta identificata e classificata l'importanza degli asset, è cruciale condurre una valutazione della vulnerabilità per ciascuna risorsa, ossia capire quanto ciascun asset è suscettibile a minacce esterne ed interne. La vulnerabilità può derivare da una serie di fattori, come:

- Obsolescenza tecnologica: L'uso di hardware e software non aggiornati o obsoleti è una delle principali cause di vulnerabilità. Le vulnerabilità conosciute in software non più supportati, per esempio, possono essere sfruttate facilmente dagli hacker.
- Errori di configurazione: Le configurazioni errate o deboli, sia a livello di rete che di software, possono aprire porte a minacce esterne. Per esempio, una configurazione errata di un firewall o un sistema di autenticazione troppo debole possono essere punti di accesso per attacchi informatici.
- Mancanza di protezioni di sicurezza: L'assenza di crittografia dei dati, autenticazione multi-fattore, backup regolari o di sistemi di monitoraggio attivi può aumentare il rischio di compromissione degli asset aziendali. La sicurezza fisica, come l'accesso non autorizzato ai server, è altrettanto importante.
- Minacce interne: Le vulnerabilità non provengono solo dall'esterno, ma anche da minacce interne, come la negligenza o l'intenzionalità di dipendenti malintenzionati, che possono compromettere la sicurezza dei dati o dei sistemi aziendali.

5.3.4 Classificazione del Rischio degli Asset

Una volta che gli asset sono mappati e le vulnerabilità sono identificate, è importante classificare il rischio associato ad ogni asset in base a probabilità e impatto. Questo processo aiuta a stabilire le priorità per l'attuazione di misure di protezione. La classificazione del rischio è generalmente realizzata attraverso:

- Gradi di probabilità: Valutare la probabilità che una minaccia possa concretizzarsi su ciascun asset, basandosi su fattori come l'esposizione alla rete, la presenza di vulnerabilità note e la frequenza degli attacchi.
- Impatto del rischio: Determinare quanto grave sarebbe il danno per l'organizzazione se l'asset fosse compromesso. L'impatto può essere economico, reputazionale, legale o operativo, a seconda della natura dell'asset.

Una volta che gli asset sono classificati all'interno delle matrici predisposte sul portale Formalize, l'azienda può concentrare le risorse e gli investimenti nelle aree più critiche, proteggendo prima gli asset ad alto rischio e a elevato impatto.

5.3.5 Strategie di Protezione degli Asset ICT

Dopo aver identificato gli asset, valutato la loro importanza e analizzato la vulnerabilità, le organizzazioni devono implementare una serie di **strategie di protezione** per mitigare i rischi associati:

- **Protezione perimetrale**: L'uso di firewall e tecnologie di crittografia per proteggere le reti aziendali e i dati da accessi non autorizzati.
- **Gestione degli accessi**: Implementazione di controlli di accesso rigorosi e politiche di gestione degli utenti per limitare l'accesso ai dati sensibili e ai sistemi critici solo a personale autorizzato.
- **Backup e disaster recovery**: Creazione di copie di sicurezza regolari dei dati e dei sistemi aziendali per garantire che, in caso di attacco o guasto, le operazioni possano essere ripristinate rapidamente.
- **Formazione e consapevolezza del personale**: Il personale deve essere formato in modo continuo per riconoscere potenziali minacce e adottare comportamenti sicuri nell'utilizzo degli asset ICT, come l'uso di password sicure e l'adozione di misure di protezione nei dispositivi mobili.

Ogni asset, che sia hardware, software, rete o base dati, deve essere mappato e valutato in base alla sua importanza e vulnerabilità, per garantire che le risorse critiche siano protette adeguatamente. Un approccio olistico alla gestione degli asset ICT permette di identificare i rischi, stabilire priorità nella protezione e implementare misure preventive efficaci per mantenere al sicuro le risorse aziendali.

5.4 Identificazione delle operazioni e degli asset: processi

L'identificazione dei processi operativi è una fase importante nella gestione dei rischi aziendali, poiché consente di esaminare attentamente i flussi di lavoro e le operazioni quotidiane per individuare i punti critici e i potenziali rischi che potrebbero compromettere la continuità e l'efficacia dell'organizzazione. Ogni processo aziendale ha un impatto diretto sulla produttività, sull'efficienza e sulla capacità dell'impresa di raggiungere i suoi obiettivi strategici. Pertanto, una valutazione accurata dei processi operativi permette non solo di identificare le risorse necessarie per la loro realizzazione, ma anche di individuare le vulnerabilità e implementare le misure di protezione adeguate per mitigarle.

5.4.1 Mappatura dei Processi Operativi

La prima fase di questa attività consiste nella mappatura dei **processi operativi aziendali**. Questa mappatura è fondamentale per comprendere come i diversi flussi di lavoro si intrecciano e quali risorse (sia tecnologiche che umane) sono coinvolte. Ogni processo deve essere analizzato in dettaglio, documentando:

- **Obiettivi del processo**: Qual è lo scopo del processo e come contribuisce al raggiungimento degli obiettivi aziendali?
- **Input e Output**: Quali risorse (materiali, dati, informazioni) sono necessarie per avviare il processo e quali sono i risultati attesi?
- **Attività e fasi**: Ogni fase del processo deve essere descritta, includendo le azioni eseguite e i responsabili.
- **Tempi e scadenze**: La durata di ogni fase e i tempi di esecuzione.
- **Tecnologie e sistemi utilizzati**: Quali strumenti, software, e tecnologie sono impiegati in ogni fase del processo?

Questa mappatura aiuta a visualizzare i flussi di lavoro, a identificare le risorse coinvolte e a comprendere meglio i legami tra i vari processi aziendali. Permette anche di rilevare potenziali aree di miglioramento e di analizzare l'efficienza dei processi.

5.4.2 Identificazione dei Punti Critici nei Processi

Una volta mappato l'intero ciclo operativo, il passo successivo è l'identificazione dei punti critici. Questi sono i momenti o le aree dove il processo potrebbe essere vulnerabile o dove potrebbero verificarsi interruzioni, errori o inefficienze significative che potrebbero compromettere la continuità delle operazioni aziendali. I principali punti critici da considerare includono:

- **Interruzione dei flussi di lavoro**: Analizzare i punti in cui i processi potrebbero essere interrotti da guasti tecnologici, errori umani o eventi esterni (come interruzioni della rete o problemi legati alla supply chain).
- **Collo di bottiglia**: Identificare i momenti in cui il flusso delle operazioni rallenta a causa di una carenza di risorse, di capacità di produzione o di tempo, generando inefficienze.
- **Rischio di errore umano**: In ogni processo ci sono momenti in cui la gestione manuale può introdurre errori o imprecisioni. L'analisi deve individuare queste aree e suggerire come ridurre il rischio di errore.
- **Dipendenza da risorse critiche**: Alcuni processi potrebbero dipendere da risorse specifiche, come competenze particolari, tecnologie avanzate o materiali difficili da reperire. La disponibilità o l'affidabilità di queste risorse deve essere costantemente monitorata.
- **Compliance e regolamenti**: In alcuni casi, i processi potrebbero essere a rischio di non conformità alle normative di settore, come le leggi sulla protezione dei dati (GDPR) o quelle sulla sicurezza informatica (NIS2). È fondamentale esaminare questi aspetti per evitare sanzioni legali e danni reputazionali.

5.4.3 Valutazione dei Potenziali Rischi nei Processi Operativi

Dopo aver identificato i punti critici, è necessario procedere con una valutazione dei rischi per determinare la probabilità che tali criticità possano effettivamente manifestarsi e l'impatto che potrebbero avere sull'organizzazione. Questo approccio prevede:

- **Analisi della probabilità**: Ogni punto critico viene analizzato in termini di probabilità di accadimento, utilizzando dati storici, esperienza pregressa e valutazioni basate su scenari

ipotetici. Ad esempio, se un certo software di gestione dei dati ha mostrato segnali di instabilità in passato, è possibile valutare una maggiore probabilità di guasto.
- Analisi dell'impatto: Viene poi valutato l'impatto che un possibile fallimento o un'interruzione potrebbe avere sull'intera operazione aziendale. L'impatto può essere finanziario, operativo, reputazionale o legato alla non conformità normativa.
- Rischio complessivo: Combinando la probabilità e l'impatto, si calcola il rischio complessivo per ogni processo, che aiuterà a determinare le priorità per l'intervento e la protezione.

5.4.4 Sviluppo di Controlli e Misure di Protezione

I controlli sono progettati per ridurre la probabilità che si verifichino eventi dannosi e per limitare l'impatto nel caso in cui tali eventi accadano.

- Automazione e digitalizzazione: L'automazione dei processi critici riduce il rischio di errore umano e aumenta l'efficienza. Implementare tecnologie per il monitoraggio continuo dei processi può anche facilitare l'identificazione tempestiva di problemi.
- Ridondanza e backup: Creare sistemi ridondanti e piani di backup per garantire la continuità operativa in caso di guasti tecnici o interruzioni dei flussi di lavoro. Ad esempio, avere più fornitori per materiali critici o infrastrutture di rete alternative.
- Monitoraggio in tempo reale: L'uso di sistemi di monitoraggio per rilevare in tempo reale anomalie nei processi aziendali può consentire un intervento tempestivo. Strumenti di business intelligence, dashboard di monitoraggio e sistemi di allerta sono cruciali.
- Gestione del cambiamento: Ogni modifica o aggiornamento ai processi operativi deve essere gestito in modo controllato per minimizzare i rischi associati. La gestione del cambiamento aiuta a garantire che tutte le modifiche siano valutate e testate prima dell'implementazione.

5.4.5 Test e Simulazioni

Una parte importante della protezione dei processi operativi è la verifica periodica della resilienza attraverso test e simulazioni. Eseguiti su base regolare, questi test possono includere:

- Simulazioni di attacco: Attività di simulazione di attacchi informatici (come penetration testing) per testare la robustezza dei sistemi contro potenziali minacce esterne.
- Test di continuità operativa: Esecuzione di piani di continuità operativa per verificare che i processi possano essere ripristinati rapidamente dopo un'interruzione. Questi test possono includere scenari come la perdita di un sistema critico o un'interruzione della catena di approvvigionamento.

L'analisi dei processi operativi è essenziale per individuare i punti critici e i potenziali rischi che potrebbero compromettere la continuità aziendale. Una corretta identificazione, valutazione e protezione di questi processi aiuta l'organizzazione a sviluppare una resilienza operativa che non solo protegge da eventi imprevisti, ma assicura anche che l'azienda possa continuare a operare senza interruzioni, aumentando la sua competitività e riducendo i rischi di danni significativi.

6. Gestione del Rischio

Questa sezione riguarda l'attuazione pratica delle strategie per identificare, valutare e mitigare i rischi ICT. Una gestione efficace del rischio consente all'organizzazione di essere preparata ad affrontare potenziali minacce alla sicurezza e alla continuità operativa. L'approccio adottato mira a garantire che le attività critiche non subiscano interruzioni significative e che i dati sensibili siano protetti da accessi non autorizzati, malfunzionamenti o attacchi esterni.

6.1 Configurazione di Formalize

L'impostazione e la personalizzazione del software Formalize sono fasi fondamentali per supportare la gestione e la documentazione dei rischi ICT. La configurazione di questo strumento prevede attività specifiche finalizzate a massimizzare l'efficienza e la precisione nella rilevazione e monitoraggio dei rischi.

- **Definizione dei parametri di monitoraggio:** Impostazione delle metriche chiave per la valutazione dei rischi, tra cui la frequenza degli eventi e l'entità dell'impatto.
- **Personalizzazione delle soglie di rischio:** Adattamento delle soglie di allerta in base alle esigenze e alle caratteristiche dell'organizzazione.
- **Integrazione con sistemi aziendali:** Collegamento del software con le piattaforme già in uso per ottenere dati aggiornati in tempo reale.
- **Formazione del personale:** Addestramento dei responsabili per l'utilizzo efficace di Formalize e la corretta interpretazione dei dati.
- **Verifica e validazione della configurazione:** Controllo iniziale per assicurare che il sistema risponda adeguatamente agli obiettivi di gestione del rischio.

6.2 Fonti di Rischio ICT e valutazione del Rischio

Questa fase identifica le diverse fonti di rischio, sia interne che esterne, che potrebbero influire sui sistemi ICT aziendali. La valutazione dei rischi consente di classificare e prioritizzare le minacce in base alla probabilità di accadimento e all'impatto potenziale sull'organizzazione.

- **Rischi interni:** Errori umani, guasti hardware, vulnerabilità nei software utilizzati e pratiche operative scorrette.
- **Rischi esterni:** Cyber attacchi, interruzioni della fornitura di servizi essenziali, modifiche normative e disastri naturali.
- **Classificazione dei rischi:** Categorizzazione dei rischi in base alla gravità e alla probabilità, per stabilire le priorità di intervento.
- **Valutazione quantitativa e qualitativa:** Uso di metriche numeriche e giudizi esperti per analizzare la portata dei rischi.
- **Creazione di un registro dei rischi:** Documentazione dettagliata dei rischi identificati, utile per la pianificazione di azioni preventive e correttive.

6.3 Trigger sulla valutazione del Rischio

È essenziale stabilire criteri chiari che attivino una rivalutazione dei rischi. Questi trigger sono fondamentali per garantire che la gestione del rischio rimanga aggiornata e reattiva rispetto ai cambiamenti interni ed esterni.

- **Modifiche infrastrutturali:** Aggiornamenti hardware o software che potrebbero introdurre nuove vulnerabilità.
- **Aggiornamenti normativi:** Cambiamenti nelle leggi o nei regolamenti che richiedono un adeguamento delle misure di sicurezza.
- **Eventi avversi:** Incidenti informatici o segnalazioni di tentativi di intrusione che suggeriscono una revisione urgente delle valutazioni.
- **Feedback dalle verifiche periodiche:** Risultati degli audit o delle simulazioni che indicano la necessità di aggiornamenti.
- **Innovazioni tecnologiche:** Introduzione di nuove tecnologie che potrebbero influire sul profilo di rischio complessivo.

6.4 Revisione del rischio e degli inventari

Il controllo periodico dei rischi identificati e degli asset aziendali è essenziale per mantenere un quadro aggiornato delle vulnerabilità e delle risorse ICT. L'inventario delle risorse deve essere costantemente allineato alle valutazioni di rischio per garantire un'efficace gestione delle minacce.

- **Aggiornamento dell'inventario ICT:** Revisione regolare dell'elenco delle risorse hardware e software presenti in azienda.
- **Verifica della criticità degli asset:** Identificazione delle risorse critiche per la continuità operativa e valutazione della loro esposizione ai rischi.
- **Controlli di conformità:** Valutazione del rispetto delle politiche aziendali e delle normative vigenti.
- **Azioni correttive e preventive:** Implementazione di misure per mitigare i rischi individuati e prevenire l'insorgenza di nuove vulnerabilità.
- **Documentazione e tracciabilità:** Registrazione di tutte le modifiche effettuate sugli asset e sulle misure di mitigazione per garantire trasparenza e responsabilità.

7. Protezione delle risorse rilevanti

La protezione delle risorse aziendali critiche costituisce un pilastro fondamentale per la salvaguardia dell'integrità, della disponibilità e della riservatezza delle informazioni e dei sistemi ICT. In un contesto caratterizzato da minacce informatiche sempre più sofisticate, garantire la sicurezza delle risorse è essenziale per mantenere la continuità operativa e la fiducia dei clienti e degli stakeholder. Questa sezione descrive le politiche, le procedure e le misure tecniche adottate per proteggere le risorse aziendali, articolandosi in monitoraggio continuo, definizione delle politiche, gestione delle operazioni ICT, sicurezza di rete, gestione degli accessi e delle identità, utilizzo della crittografia e supervisione dei progetti tecnologici.

7.1 Protezione delle risorse rilevanti: monitoraggio

Il monitoraggio delle risorse ICT è cruciale per individuare tempestivamente comportamenti anomali e potenziali minacce alla sicurezza. L'azienda adotta un sistema di monitoraggio continuo che garantisce la sorveglianza costante delle infrastrutture critiche, dei sistemi operativi e delle applicazioni in uso. Questa attività si basa sull'analisi dei log generati dai dispositivi di rete, dai server e dai sistemi di sicurezza, consentendo di tracciare tutte le operazioni e rilevare eventuali anomalie.

Inoltre, sono implementati sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) che analizzano il traffico di rete in tempo reale, identificando tentativi di accesso non autorizzati o movimenti sospetti. Il monitoraggio non si limita alle risorse digitali: l'azienda ha introdotto anche misure di sorveglianza fisica, come il controllo degli accessi ai locali sensibili e la videosorveglianza delle aree a rischio. La combinazione di questi strumenti permette un controllo a 360 gradi, riducendo il rischio di interruzioni operative e attacchi informatici.

7.2 Politiche

Le politiche aziendali rappresentano la base su cui si fondano tutte le attività di sicurezza informatica. Questi documenti stabiliscono le regole per l'uso sicuro delle tecnologie, la gestione dei dati e la protezione delle informazioni sensibili. Ogni dipendente ha l'obbligo di conoscere e rispettare tali linee guida, che vengono regolarmente aggiornate per rispondere all'evoluzione delle minacce e ai cambiamenti normativi.

L'azienda promuove la consapevolezza e la formazione continua del personale, organizzando corsi periodici e campagne di sensibilizzazione sulla sicurezza informatica. In particolare, le politiche prevedono l'adozione di misure per la protezione dei dati personali, la gestione sicura dei dispositivi mobili e l'utilizzo corretto delle risorse aziendali. Particolare attenzione è rivolta alla gestione dei dati in cloud e all'uso di dispositivi personali (BYOD), per i quali sono state stabilite regole chiare e restrittive.

7.3 Operazioni ICT

Le operazioni quotidiane legate alle tecnologie dell'informazione devono essere gestite in modo sicuro e conforme alle politiche aziendali. Questo comporta l'adozione di procedure per la gestione dei sistemi, l'implementazione di aggiornamenti regolari e la verifica dell'integrità dei software. L'azienda effettua periodicamente scansioni per individuare vulnerabilità e adottare misure correttive tempestive.

Un elemento chiave è rappresentato dalla gestione dei backup: vengono eseguiti salvataggi regolari dei dati critici, archiviati in ambienti sicuri e testati per verificarne l'efficacia in caso di necessità di ripristino. Le operazioni ICT comprendono anche la gestione delle richieste di supporto tecnico e la risoluzione dei problemi operativi, garantendo che le attività aziendali possano svolgersi senza interruzioni.

7.4 Politica di Gestione della Sicurezza di Rete

La rete aziendale rappresenta la spina dorsale delle operazioni ICT, motivo per cui la sua protezione richiede misure specifiche. L'azienda ha adottato una politica di sicurezza di rete che prevede controlli perimetrali mediante firewall e sistemi di filtraggio, volti a bloccare traffico non autorizzato e potenziali attacchi.

La segmentazione della rete consente di isolare le aree critiche, limitando la propagazione di eventuali minacce e facilitando la gestione degli accessi. Il monitoraggio del traffico di rete permette di individuare comportamenti anomali e prevenire attacchi informatici. Per quanto riguarda gli accessi remoti, è previsto l'utilizzo di connessioni VPN sicure, supportate da sistemi di autenticazione a più fattori (MFA), per garantire che solo personale autorizzato possa accedere alle risorse aziendali da postazioni esterne.

7.5 Politica di gestione degli accessi e delle identità

La gestione degli accessi e delle identità è fondamentale per prevenire l'uso improprio delle risorse aziendali. La politica adottata stabilisce criteri rigorosi per l'assegnazione dei permessi, basati sul principio del privilegio minimo, che garantisce a ciascun utente l'accesso esclusivamente alle risorse necessarie per svolgere le proprie mansioni.

Le credenziali di accesso devono rispettare requisiti di complessità, con obbligo di aggiornamento periodico delle password. Per ridurre i rischi associati alla gestione manuale delle credenziali, l'azienda utilizza strumenti dedicati che consentono di archiviare in modo sicuro le informazioni di autenticazione. Tutti gli accessi agli asset critici vengono registrati e monitorati: eventuali tentativi di accesso non autorizzato sono oggetto di indagini immediate. In caso di cessazione del rapporto di lavoro, le credenziali vengono disattivate tempestivamente per prevenire potenziali abusi.

7.6 Politica sulla crittografia e cifratura

Per proteggere i dati sensibili, l'azienda deve una politica rigorosa sull'uso della crittografia. I dati archiviati su dispositivi aziendali e piattaforme cloud sono cifrati mediante algoritmi avanzati come AES-256, garantendo la protezione delle informazioni anche in caso di furto o smarrimento dei dispositivi.

Le comunicazioni elettroniche, comprese le e-mail e le piattaforme di messaggistica istantanea, sono protette da protocolli crittografici aggiornati (es. TLS 1.3), che impediscono l'intercettazione dei dati in transito. La gestione delle chiavi crittografiche segue procedure rigorose: le chiavi sono generate, distribuite e archiviate in ambienti protetti, con sistemi di controllo che ne regolano l'uso e la revoca. L'azienda si impegna inoltre a rispettare le normative vigenti in materia di protezione dei dati e a monitorare le evoluzioni tecnologiche per garantire l'adozione delle soluzioni più sicure.

7.7 Gestione dei progetti ICT

La gestione dei progetti tecnologici deve garantire che ogni iniziativa sia conforme alle politiche di sicurezza e ai principi di gestione del rischio. Già nella fase di pianificazione, viene effettuata un'analisi dei rischi ICT per identificare potenziali criticità e adottare misure preventive. I progetti vengono costantemente monitorati e sottoposti a verifiche per assicurare che rispettino i requisiti di sicurezza stabiliti.

Durante la fase di implementazione, vengono eseguiti test di sicurezza, tra cui penetration test e vulnerability assessment, per individuare eventuali vulnerabilità prima del rilascio definitivo. La documentazione dei progetti include manuali operativi e procedure di emergenza, utili per garantire la continuità dei servizi anche in situazioni critiche. Infine, viene prevista una formazione specifica per gli utenti finali, al fine di favorire una corretta adozione delle nuove tecnologie e ridurre i rischi legati a errori umani o uso improprio delle risorse implementate.

8. Gestione degli incidenti legati alle ICT

Questa sezione descrive le procedure da adottare per prevenire, rilevare, rispondere e recuperare dagli incidenti ICT. Una gestione efficace degli incidenti riduce l'impatto delle minacce sulla continuità aziendale.

8.1 Team per la Gestione degli Incidenti di Sicurezza Informatica

La creazione di un team dedicato alla gestione degli incidenti ICT è un elemento imprescindibile per garantire una risposta coordinata e tempestiva. Questo team deve essere composto da figure professionali dotate di competenze specialistiche e con ruoli chiaramente definiti, per evitare ambiguità durante la gestione dell'emergenza. I principali ruoli previsti sono:

- **Responsabile del team:** Supervisiona l'intero processo di gestione dell'incidente, prendendo decisioni strategiche e garantendo che le risposte siano adeguate e tempestive.
- **Analisti di sicurezza:** Indagano sulle cause e le modalità di attacco, effettuando un'analisi approfondita delle vulnerabilità sfruttate.
- **Specialisti ICT:** Intervengono sul piano tecnico per contenere l'incidente, ripristinare i sistemi e implementare misure correttive.
- **Referente per la comunicazione:** Cura la diffusione delle informazioni interne ed esterne, assicurando che i messaggi siano chiari, accurati e coerenti.
- **Supporto legale e compliance:** Valuta gli obblighi normativi derivanti dall'incidente e fornisce indicazioni per le comunicazioni verso le autorità competenti.

Il team deve essere costantemente aggiornato attraverso sessioni di formazione e simulazioni pratiche, in modo da affinare le proprie capacità e mantenere un elevato livello di prontezza operativa.

8.2 Documentazione sulla gestione degli incidenti legati alle ICT

Una documentazione dettagliata è essenziale per gestire gli incidenti in modo sistematico ed efficace. Deve essere facilmente accessibile a tutto il personale coinvolto e costantemente aggiornata per riflettere le evoluzioni tecnologiche e normative. I principali documenti includono:

- **Procedure operative standard (SOP):** Linee guida passo-passo per affrontare i diversi tipi di incidenti, dalla loro identificazione fino alla chiusura.
- **Moduli di segnalazione:** Strumenti pratici per raccogliere informazioni dettagliate e standardizzate sugli incidenti, facilitando l'analisi e la risposta.
- **Registro degli incidenti:** Archivio centralizzato dove vengono tracciati tutti gli eventi, le azioni intraprese e i tempi di risposta, utile anche per future revisioni e audit.
- **Check-list di controllo:** Elenchi operativi che supportano i team durante la gestione degli incidenti, evitando dimenticanze o errori procedurali.

Aggiornare costantemente la documentazione permette di trarre vantaggio dalle esperienze pregresse e di prevenire la ripetizione degli stessi errori.

8.3 Meccanismi di rilevazione degli incidenti

La capacità di individuare tempestivamente le anomalie è fondamentale per limitare l'impatto di un incidente. L'organizzazione deve adottare una combinazione di strumenti tecnologici e processi umani, tra cui:

- Sistemi di rilevamento delle intrusioni (IDS) e prevenzione (IPS): Monitorano in tempo reale il traffico di rete, segnalando comportamenti sospetti o tentativi di attacco.
- Piattaforme SIEM (Security Information and Event Management): Raccolgono e analizzano dati provenienti da diverse fonti, permettendo di individuare minacce complesse attraverso la correlazione degli eventi.
- Monitoraggio dei log: Controllo sistematico dei registri di sistema, applicazioni e dispositivi per rilevare attività anomale o non autorizzate.
- Formazione del personale: Gli utenti sono spesso la prima linea di difesa; sensibilizzarli sui comportamenti a rischio e sulle modalità di segnalazione può prevenire numerosi incidenti.
- Monitoraggio proattivo delle vulnerabilità: Scansioni periodiche dei sistemi per identificare punti deboli prima che possano essere sfruttati da attori malintenzionati.

8.4 Classificazione degli incidenti

Attribuire un livello di gravità agli incidenti è fondamentale per stabilire le priorità di intervento e allocare correttamente le risorse. La classificazione può basarsi su criteri quali l'impatto sui servizi, la diffusione dell'incidente e le conseguenze legali o reputazionali. Si possono individuare i seguenti livelli:

- Basso: Eventi con impatto limitato e nessuna interruzione dei servizi. Richiedono monitoraggio ma non interventi urgenti.
- Moderato: Incidenti che potrebbero compromettere temporaneamente alcune funzioni aziendali senza conseguenze gravi a lungo termine.
- Alto: Situazioni che causano disservizi significativi, perdita di dati o violazioni di sicurezza rilevanti. Richiedono un intervento immediato.
- Critico: Incidenti che mettono a rischio la continuità operativa, la sicurezza delle informazioni e la reputazione aziendale. Necessitano di una gestione prioritaria e coinvolgono il management di alto livello.

8.5 Classificazione delle minacce informatiche

Una mappatura chiara delle minacce consente di predisporre difese mirate e misure preventive efficaci. Le categorie principali includono:

- Malware: Programmi dannosi come virus, worm, trojan e ransomware, progettati per danneggiare i sistemi o estorcere denaro.
- Phishing e social engineering: Tecniche di manipolazione psicologica finalizzate a carpire informazioni sensibili, spesso tramite email o telefonate ingannevoli.

- **Accessi non autorizzati:** Tentativi di violazione dei sistemi informatici per rubare dati o compromettere le operazioni.
- **Attacchi DDoS (Distributed Denial of Service):** Operazioni coordinate che mirano a saturare le risorse di sistema, rendendo i servizi indisponibili.
- **Sfruttamento di vulnerabilità note:** Attacchi che approfittano di sistemi non aggiornati o configurati in modo errato.

8.6 Segnalazione

Un processo di segnalazione rapido e strutturato è essenziale per contenere i danni derivanti da un incidente. Gli elementi chiave includono:

- **Canali dedicati e facilmente accessibili:** Email, hotline e piattaforme online devono essere sempre operative e accessibili al personale.
- **Tempi di risposta definiti:** Stabilire delle metriche (SLA) per garantire che ogni segnalazione venga presa in carico entro tempi stabiliti in base alla gravità.
- **Procedure chiare per la segnalazione:** I dipendenti devono sapere come, quando e a chi segnalare un potenziale incidente.
- **Comunicazione bidirezionale:** È importante che chi segnala riceva aggiornamenti sull'evoluzione e la gestione dell'incidente.

8.7 Revisione post-incidente

La revisione post-incidente è un momento cruciale per apprendere dalle situazioni di crisi e migliorare la resilienza organizzativa. Le attività previste comprendono:

- **Analisi delle cause profonde (Root Cause Analysis):** Indagine dettagliata per individuare le origini dell'incidente e le eventuali falle nei processi.
- **Redazione di un report dettagliato:** Documento che descrive le fasi dell'incidente, le azioni intraprese, i tempi di reazione e le raccomandazioni future.
- **Sessioni di debriefing:** Incontri tra i membri del team e le parti coinvolte per discutere l'accaduto e definire azioni correttive.
- **Aggiornamento delle procedure:** In base ai risultati dell'analisi, è fondamentale modificare le SOP e la documentazione correlata per evitare il ripetersi dell'incidente.

8.8 Segnalazione delle modifiche post-incidente

Le modifiche apportate ai sistemi o alle procedure a seguito di un incidente devono essere documentate con cura per garantire tracciabilità e trasparenza. La documentazione deve includere:

- Descrizione dettagliata delle modifiche implementate.
- Motivazioni che hanno reso necessarie tali modifiche.
- Analisi dell'impatto previsto sui sistemi e sulle operazioni.
- Approvazioni da parte delle figure autorizzate.
- Aggiornamento dei registri e delle procedure interne.

8.9 Piani di comunicazione

La comunicazione durante un incidente è fondamentale per gestire la percezione esterna e mantenere la fiducia degli stakeholder. Un piano di comunicazione efficace deve prevedere:

- Messaggi predefiniti e adattabili alle varie situazioni.
- Procedure per la gestione dei contatti con i media e con i clienti.
- Linee guida per la comunicazione interna, per garantire che tutto il personale riceva istruzioni chiare.
- Adempimenti normativi per la notifica alle autorità competenti entro i termini previsti.
- Canali alternativi in caso di indisponibilità delle consuete vie di comunicazione.

8.10 Ruoli di comunicazione

Per garantire che le comunicazioni siano tempestive e coerenti, è essenziale assegnare ruoli ben definiti:

- **Portavoce ufficiale:** Interagisce con i media e rilascia dichiarazioni pubbliche, assicurando una comunicazione trasparente e controllata.
- **Responsabile delle comunicazioni interne:** Coordina la diffusione delle informazioni ai dipendenti, evitando disinformazione e confusione.
- **Referente legale:** Verifica che tutte le comunicazioni rispettino le normative vigenti e gestisce i rapporti con le autorità di regolamentazione.
- **Responsabile IT:** Fornisce aggiornamenti tecnici e supporta la comunicazione con informazioni precise e aggiornate sull'incidente.

8.11 Test del piano di comunicazione

Verificare l'efficacia del piano di comunicazione è fondamentale per prepararsi a gestire incidenti reali. I test devono essere svolti regolarmente e possono includere:

- **Simulazioni pratiche con scenari realistici:** Coinvolgono tutti i soggetti interessati e permettono di identificare punti deboli e margini di miglioramento.
- **Valutazione dei tempi di reazione:** Misurare la rapidità con cui le informazioni vengono raccolte e diffuse durante l'incidente simulato.
- **Feedback dei partecipanti:** Raccogliere osservazioni e suggerimenti per ottimizzare i processi comunicativi.
- **Aggiornamento delle procedure:** Apportare modifiche basate sui risultati delle simulazioni per garantire un miglioramento continuo.

9. Continuità Operativa

Il Digital Operational Resilience Act (DORA) pone una forte enfasi sulla continuità operativa come elemento centrale per garantire la resilienza digitale delle istituzioni finanziarie e dei fornitori di servizi ICT. Il rispetto di tali requisiti non solo consente alle organizzazioni di far fronte a potenziali interruzioni operative, ma rafforza anche la loro capacità di prevenire, gestire e riprendersi efficacemente da eventi dirompenti. Di seguito vengono approfonditi i principali elementi previsti dal protocollo DORA riguardanti la continuità operativa.

9.1 La continuità operativa come responsabilità dell'Organo di Gestione

L'organo di gestione detiene la responsabilità ultima nell'assicurare la continuità delle operazioni. Questo implica l'approvazione, il monitoraggio e la revisione periodica delle strategie e delle misure adottate per la gestione delle interruzioni. L'integrazione della continuità operativa nella governance aziendale è cruciale per garantire l'allineamento con la strategia complessiva e con il sistema di gestione dei rischi.

Le principali responsabilità dell'organo di gestione includono:

- Approvare la politica aziendale di continuità operativa e i piani correlati.
- Supervisionare le attività di implementazione e test dei piani di continuità.
- Assicurare che le risorse (umane, tecnologiche e finanziarie) siano adeguate per sostenere la resilienza operativa.
- Promuovere una cultura organizzativa orientata alla prevenzione e alla gestione delle crisi.

9.2 Team per la Continuità Operativa

La creazione di un team dedicato alla continuità operativa rappresenta un pilastro fondamentale per l'attuazione efficace delle misure previste dal DORA. Questo gruppo deve essere costituito da rappresentanti delle principali funzioni aziendali e supportato da specialisti in gestione del rischio, tecnologia e comunicazione.

Responsabilità principali del team:

- Coordinare le attività durante le situazioni di crisi.
- Assicurare che le funzioni aziendali coinvolte siano pronte ad attuare le misure previste.
- Garantire una formazione continua per accrescere la preparazione del personale.
- Mantenere attiva una comunicazione interna efficace per ridurre i tempi di inattività.

9.3 Documentazione relativa alla Continuità Operativa

Una documentazione accurata e aggiornata è fondamentale per garantire risposte operative coerenti e tempestive. I documenti devono includere:

- Politiche e procedure per la gestione della continuità.
- Manuali operativi specifici per ogni funzione critica.
- Guide pratiche per la risposta agli incidenti e piani di ripristino.

Requisiti essenziali:

- Accessibilità facilitata per tutte le parti interessate.
- Aggiornamenti periodici per riflettere modifiche organizzative e tecnologiche.
- Archiviazione sicura per garantire la disponibilità in caso di emergenza.

9.4 Business Impact Assessment

Comprendere quali siano i processi fondamentali per la propria organizzazione e valutarne la vulnerabilità è il primo passo per garantire una solida continuità operativa. È proprio questo l'obiettivo del **Business Impact Assessment (BIA)**, uno strumento che consente di individuare le attività critiche e le dipendenze tra i vari reparti o sistemi. Attraverso il BIA, l'organizzazione acquisisce consapevolezza delle conseguenze derivanti da eventuali interruzioni e può così stabilire le priorità di ripristino. Ciò significa definire quali funzioni devono essere riprese per prime e in quali tempi, assicurandosi che i tempi massimi di inattività accettabili siano compatibili con le esigenze dei clienti e delle normative di settore. Il BIA, dunque, non si limita a essere un documento statico, ma rappresenta una guida operativa per prendere decisioni consapevoli e tempestive durante le emergenze.

9.5 Piano di Continuità Operativa e Piano di Risposta e Ripristino

Quando si verifica un evento imprevisto, come un guasto informatico o un'interruzione nella catena di fornitura, è fondamentale sapere esattamente cosa fare, chi coinvolgere e quali risorse attivare. È qui che entrano in gioco il **Piano di Continuità Operativa (BCP)** e i **Piani di Risposta e Ripristino**. Questi strumenti devono essere chiari, pratici e facilmente consultabili. Devono illustrare le azioni da intraprendere per garantire la prosecuzione dei servizi essenziali anche in condizioni avverse, delineando le responsabilità di ciascun membro del team. È essenziale che tali piani siano allineati con le informazioni emerse dal BIA, così da intervenire rapidamente sulle aree più vulnerabili e limitare l'impatto operativo, finanziario e reputazionale. Un piano ben strutturato permette di ridurre lo stress operativo nei momenti di crisi e di accelerare il ritorno alla normalità, evitando improvvisazioni che potrebbero aggravare la situazione.

9.6 Test BCP sulla continuità operativa e dei piani di risposta

Un piano, per quanto ben elaborato, perde efficacia se non viene messo alla prova. Ecco perché è indispensabile svolgere test periodici sui piani di continuità operativa e sui piani di risposta e ripristino. Questi test non devono essere considerati semplici formalità, ma vere e proprie simulazioni di scenari realistici, in cui il personale può esercitarsi a gestire situazioni di emergenza. Immaginare, ad esempio, una simulazione di blackout o di attacco informatico consente di individuare in anticipo eventuali punti deboli e correggerli prima che si verifichi un evento reale. Coinvolgere anche i fornitori di servizi critici è altrettanto importante, poiché la resilienza dell'organizzazione dipende spesso dall'intera catena operativa. Ogni test dovrebbe concludersi con un report dettagliato che evidenzi le criticità riscontrate e suggerisca azioni correttive, così da trasformare l'esperienza simulata in un'occasione di miglioramento concreto.

9.7 Revisione del piano di continuità operativa (BCP) e dei piani di risposta

La revisione periodica dei piani deve avvenire:

- Almeno una volta all'anno.
- Ogni volta che si verificano cambiamenti significativi nell'organizzazione, nei processi o nella tecnologia.

L'obiettivo è garantire che le misure adottate rimangano pertinenti ed efficaci rispetto al contesto operativo e alle minacce emergenti.

9.8 Lezioni apprese

Ogni crisi o esercitazione rappresenta un'opportunità per imparare e migliorare. L'analisi delle lezioni apprese è un momento cruciale per riflettere su cosa ha funzionato e cosa, invece, può essere ottimizzato. Dopo un test o un evento reale, raccogliere feedback dai partecipanti permette di avere una visione completa delle dinamiche operative e decisionali. Spesso emergono suggerimenti pratici che possono fare la differenza durante un'emergenza reale: ad esempio, la necessità di semplificare una procedura troppo complessa o di migliorare la comunicazione interna. Documentare queste esperienze consente di aggiornare i piani in modo mirato e di rafforzare la cultura aziendale orientata alla prevenzione. È fondamentale che le lezioni apprese non restino solo sulla carta, ma si traducano in azioni concrete per aumentare la resilienza complessiva dell'organizzazione.

9.9 Documentazione

L'intera documentazione deve essere:

- Archiviata in modo sicuro ma facilmente accessibile alle figure responsabili.
- Organizzata in modo logico per facilitare la consultazione rapida.
- Costantemente aggiornata per riflettere l'evoluzione dei processi e delle tecnologie.

La disponibilità di documenti aggiornati è essenziale per garantire una gestione efficace delle situazioni di emergenza.

9.10 Costi e perdite annuali

Monitorare i costi legati alla gestione della continuità operativa e stimare le potenziali perdite derivanti da interruzioni è cruciale per:

- Ottimizzare le risorse investite.
- Valutare il rapporto costo-beneficio delle misure adottate.
- Pianificare interventi mirati per la protezione delle attività critiche.

Attività raccomandate:

- Creare un sistema di monitoraggio dei costi diretti e indiretti.
- Confrontare le stime delle perdite con i dati storici di interruzioni passate.
- Adeguare le strategie in base all'analisi dei dati raccolti.

10. Backup, Ripristino e Recupero

La gestione dei processi di backup, ripristino e recupero è un aspetto cruciale per garantire la continuità operativa di qualsiasi organizzazione. In un contesto aziendale sempre più dipendente dalla tecnologia, la protezione e la capacità di recuperare i dati in tempi rapidi sono essenziali per ridurre i rischi legati a interruzioni impreviste, come attacchi informatici, guasti hardware, disastri naturali o errori umani. Una corretta gestione dei backup e un piano di recupero ben definito possono fare la differenza tra il ripristino immediato delle operazioni e una lunga interruzione dei servizi aziendali, con conseguenti perdite economiche e danni reputazionali. La sezione che segue si concentra sulle linee guida per implementare un piano completo di backup e recupero, articolato in dieci sotto-sezioni fondamentali per garantire un'adeguata protezione dei dati aziendali.

10.1 Documentazione

Una documentazione completa e dettagliata è la base di qualsiasi piano di backup, ripristino e recupero. La documentazione deve includere tutte le informazioni relative ai processi e alle procedure da seguire, come ad esempio le soluzioni di backup utilizzate, le modalità di conservazione dei dati, e la definizione delle responsabilità. Ogni membro del team deve avere accesso a procedure operative chiare e ben delineate, in modo da sapere come agire in caso di necessità. Inoltre, la documentazione deve essere facilmente accessibile e aggiornata regolarmente per riflettere le modifiche ai sistemi e alle tecnologie aziendali.

10.2 Attivazione e Test

Il piano di backup e recupero non è sufficiente se non viene regolarmente testato. La pianificazione di test periodici è essenziale per verificare l'efficacia delle soluzioni adottate. Durante i test, è fondamentale simulare scenari di disastro realistici per verificare la tempestività del recupero dei dati e dei sistemi. Questi test permettono di identificare eventuali debolezze nel piano, come la lentezza nelle operazioni di ripristino o la difficoltà nell'accesso ai backup, e di apportare le correzioni necessarie. La frequenza dei test dovrebbe essere stabilita in base alla criticità dei sistemi aziendali e ai rischi associati.

10.3 Requisiti dei Sistemi di Backup

I sistemi di backup devono essere progettati per garantire l'integrità e la sicurezza dei dati aziendali. Ciò implica che i backup non solo debbano essere eseguiti regolarmente, ma anche che siano protetti da tecniche avanzate di sicurezza. La cifratura dei dati, ad esempio, è una misura fondamentale per prevenire accessi non autorizzati e garantire la privacy. Inoltre, i sistemi di backup devono essere in grado di gestire l'intero volume dei dati aziendali, senza rischiare di saturare le risorse disponibili o di generare ritardi nel processo di recupero.

10.4 Ridondanza delle Capacità ICT

La ridondanza delle capacità ICT è una pratica fondamentale per evitare che un singolo punto di fallimento comprometta l'intero sistema aziendale. In caso di guasto di una componente hardware o di una parte del sistema, è essenziale che ci siano copie dei dati disponibili in altre sedi o dispositivi. La ridondanza deve essere implementata sia a livello geografico (ad esempio, utilizzando datacenter situati in diverse località) che a livello hardware, con la duplicazione dei sistemi di backup in modo da garantire la continuità dei processi aziendali anche in situazioni di emergenza.

10.5 RTO (Recovery Time Objective)

Il Recovery Time Objective (RTO) definisce il tempo massimo che un'organizzazione può tollerare per il ripristino delle proprie operazioni dopo un'interruzione. Stabilire un RTO adeguato è cruciale per limitare i tempi di inattività e ridurre al minimo l'impatto sul business. Un RTO troppo lungo potrebbe tradursi in interruzioni prolungate e costose, mentre un RTO troppo breve potrebbe risultare difficile da rispettare senza compromettere la qualità del recupero. La definizione dell'RTO dipende dalla criticità dei singoli sistemi aziendali e dalla valutazione dei rischi.

10.6 RPO (Recovery Point Objective)

Il Recovery Point Objective (RPO) è un altro parametro fondamentale per la gestione dei backup e del recupero dei dati. L'RPO definisce la quantità massima di dati che un'organizzazione è disposta a perdere in caso di disastro. Impostare un RPO chiaro aiuta a determinare la frequenza dei backup e a definire una strategia di protezione dei dati che possa minimizzare la perdita di informazioni. Un RPO più breve implica un numero maggiore di backup, aumentando la protezione ma anche i costi e la complessità operativa.

10.7 Gestione del Recupero degli Incidenti

La gestione del recupero degli incidenti riguarda la preparazione e l'implementazione di un piano di risposta strutturato per affrontare guasti, attacchi informatici o altri eventi che potrebbero compromettere i sistemi aziendali. Il piano deve includere procedure specifiche per l'identificazione, la valutazione e la gestione dei sistemi compromessi. La gestione efficace degli incidenti richiede una risposta rapida e coordinata, con l'obiettivo di ridurre al minimo i danni e ripristinare il più velocemente possibile le operazioni aziendali.

10.8 Monitoraggio Continuo

Il monitoraggio continuo dei sistemi di backup e del loro funzionamento è cruciale per garantire l'efficacia del piano di recupero. Un sistema di monitoraggio adeguato consente di rilevare tempestivamente eventuali anomalie o fallimenti nel processo di backup, come errori nelle procedure di archiviazione o malfunzionamenti nelle applicazioni di backup. Il monitoraggio proattivo aiuta a prevenire problemi prima che si trasformino in disastri, consentendo interventi tempestivi e riducendo i tempi di inattività.

10.9 Formazione del Personale

Il personale coinvolto nella gestione dei backup e del recupero dei dati deve essere adeguatamente formato per rispondere in modo efficace alle situazioni di emergenza. La formazione deve comprendere non solo la conoscenza delle procedure di recupero, ma anche l'utilizzo degli strumenti di backup, le tecniche di gestione degli incidenti e la gestione dei rischi associati alla perdita di dati. Il personale deve essere in grado di affrontare situazioni stressanti con calma e competenza, riducendo i rischi legati a errori umani durante le fasi di recupero.

10.10 Revisione e Aggiornamento Periodico

Infine, il piano di backup e recupero deve essere soggetto a revisione e aggiornamento periodico. La tecnologia evolve rapidamente e nuove minacce, come attacchi informatici sempre più sofisticati, emergono costantemente. Pertanto, è essenziale eseguire aggiornamenti annuali o ogni volta che si verificano modifiche significative nei sistemi aziendali. Questo assicura che il piano rimanga efficace e in grado di rispondere adeguatamente alle nuove sfide tecnologiche e alle minacce emergenti.

Un piano di backup e recupero ben strutturato è essenziale per la protezione dei dati aziendali e la continuità operativa. Implementando questi dieci principi fondamentali, le organizzazioni possono ridurre significativamente i rischi legati a disastri, guasti e attacchi informatici, garantendo una risposta tempestiva e efficace in caso di emergenza.

11. Digital Operational Resilience (DOR)

La Digital Operational Resilience (DOR) riguarda la capacità di un'organizzazione di continuare a operare e proteggere i propri servizi in caso di crisi, cyber-attacchi o altre interruzioni significative. Il protocollo DOR stabilisce delle linee guida per testare, verificare e rafforzare la resilienza digitale, identificando i punti critici e migliorando le capacità di risposta a incidenti. Le seguenti sottovoci esplorano gli aspetti cruciali relativi ai test di resilienza operativa digitale e alla gestione dei rischi associati.

11.1 Scopo del Test

Lo scopo del test di resilienza digitale è quello di verificare la capacità dell'organizzazione di affrontare e superare le interruzioni significative nei servizi ICT. I test permettono di identificare le vulnerabilità nei sistemi, nei processi e nelle risorse, assicurando che le misure di protezione siano efficaci. I test devono essere progettati per simulare scenari realistici e complessi, testando la resilienza dell'infrastruttura, delle persone e delle politiche aziendali.

11.2 Test sulle Specifiche Tecniche

I test sulle specifiche tecniche sono mirati a verificare che le soluzioni tecniche adottate siano in grado di resistere a stress e attacchi esterni. Questi test includono la simulazione di guasti hardware, software, e vulnerabilità delle reti, e valutano l'efficacia delle soluzioni di sicurezza implementate. Devono essere eseguiti regolarmente per garantire che l'infrastruttura ICT sia allineata alle migliori pratiche di resilienza.

11.3 Approccio al Rischio

L'approccio al rischio nell'ambito della DOR implica una valutazione continua delle minacce e dei vulnerabilità, per sviluppare strategie di protezione e recupero. Questo approccio include l'identificazione dei rischi, la valutazione della probabilità di accadimento e dell'impatto, e la definizione di misure preventive e di mitigazione. È importante che l'approccio al rischio si basi su una comprensione approfondita delle minacce emergenti, come gli attacchi informatici sofisticati.

11.4 Definizione delle Priorità

La definizione delle priorità è essenziale per focalizzare gli sforzi di resilienza sulle aree più critiche e vulnerabili. Alcuni sistemi, applicazioni e dati sono più sensibili di altri e quindi devono essere protetti e ripristinati con maggiore urgenza. La classificazione delle priorità aiuta a stabilire gli obiettivi di recupero e le risorse necessarie per garantire la continuità dei servizi più vitali.

11.5 Lezioni di Test DOR

Le lezioni apprese dai test di resilienza operativa sono fondamentali per migliorare continuamente i piani di gestione degli incidenti e di recupero. I test devono includere una fase di analisi post-incidente, durante la quale si identificano le criticità emerse, le inefficienze nei processi e le aree di miglioramento. Le lezioni apprese devono essere documentate e integrate nelle future strategie di resilienza.

11.6 KPI (Key Performance Indicators)

I KPI nella DOR misurano l'efficacia delle politiche e delle procedure implementate per garantire la resilienza digitale. Gli indicatori possono includere il tempo di recupero (RTO), la frequenza dei test di resilienza, il tasso di successo nel ripristino dei dati, e la risposta a incidenti. I KPI devono essere monitorati regolarmente per valutare se l'organizzazione sta raggiungendo gli obiettivi di resilienza e per fare gli aggiustamenti necessari.

11.7 DOR: Formazione

La formazione è un elemento fondamentale per garantire che il personale sia preparato a rispondere efficacemente a incidenti e interruzioni. I programmi di formazione devono coprire la gestione delle emergenze, la sicurezza informatica, la gestione del rischio e l'uso degli strumenti di recupero. La formazione continua aiuta a mantenere alta la consapevolezza dei dipendenti riguardo alla resilienza digitale e a migliorare la capacità di risposta durante le crisi.

11.8 Test di Penetrazione Avanzati Basati sulle Minacce (TLPT)

I Test di Penetrazione Avanzati Basati sulle Minacce (TLPT) sono test di sicurezza che simulano attacchi complessi da parte di hacker, utilizzando tecniche avanzate per identificare vulnerabilità inaspettate. Questi test vanno oltre i tradizionali test di penetrazione, cercando di emulare minacce reali e sofisticate per valutare come i sistemi aziendali possano resistere ad attacchi avanzati, e per migliorare le difese.

11.8.1 L'Obiettivo dei TLPT nel Quadro DORA

I TLPT, all'interno del DORA, hanno l'obiettivo di valutare la capacità di un'organizzazione di resistere a minacce informatiche avanzate simulando attacchi reali che potrebbero compromettere la continuità operativa e la sicurezza dei dati. A differenza dei tradizionali test di penetrazione, che si concentrano su vulnerabilità note e su una verifica generale della sicurezza, i TLPT riproducono scenari di attacco mirati, sofisticati e persistenti, tipici delle minacce attuali nel settore finanziario.

L'implementazione di questi test è particolarmente rilevante per le entità finanziarie critiche, tra cui banche, assicurazioni, borse e infrastrutture di mercato, che devono dimostrare un'elevata capacità di risposta agli attacchi cyber e una strategia efficace di difesa.

11.8.2 Fasi di un TLPT nel Contesto DORA

1. **Definizione del perimetro**: dentificazione delle risorse e dei sistemi critici da testare, basata sull'analisi dei rischi e sull'intelligence sulle minacce.
2. **Raccolta di informazioni (OSINT & Reconnaissance)**: Analisi delle superfici di attacco disponibili, identificazione delle vulnerabilità e preparazione del test sulla base di scenari di minaccia realistici.
3. **Simulazione dell'attacco**: Utilizzo di tecniche avanzate (es. exploit zero-day, social engineering, attacchi supply chain) per verificare le difese dell'organizzazione.
4. **Analisi dei risultati**: Valutazione dell'impatto potenziale, documentazione delle vulnerabilità critiche e suggerimenti per migliorare la resilienza.
5. **Piani di remediation e follow-up**: Implementazione di misure correttive e miglioramento delle strategie di cybersecurity sulla base delle evidenze emerse dal test.

11.8.3 Benefici per la Conformità a DORA

L'identificazione delle vulnerabilità critiche prima che possano essere sfruttate da attaccanti reali è un aspetto fondamentale dei Test di Penetrazione Avanzati Basati sulle Minacce (TLPT). Questi test aiutano a scoprire debolezze che potrebbero essere trascurate durante analisi di sicurezza tradizionali, riducendo così il rischio di attacchi futuri. Inoltre, i TLPT contribuiscono al miglioramento della risposta agli incidenti e della resilienza operativa. Testando gli scenari di attacco più complessi, le organizzazioni possono affinare i propri piani di risposta, garantendo una gestione più rapida ed efficace di eventuali incidenti informatici.

Questi test aumentano anche la consapevolezza e la preparazione dell'organizzazione rispetto alle minacce avanzate. Permettono ai team di sicurezza di capire meglio come gli attaccanti possano approfittare delle vulnerabilità e di prendere misure preventive per proteggere i sistemi in modo più proattivo.

L'integrazione dei TLPT nel quadro del DORA rappresenta un passo essenziale per rafforzare la sicurezza informatica e la resilienza delle istituzioni finanziarie. Le aziende del settore devono adottare un approccio strategico e proattivo per garantire che questi test siano condotti in modo efficace, consentendo di affrontare minacce emergenti e migliorare continuamente le difese aziendali.

11.9 Risultati del TLPT

I risultati del TLPT forniscono una panoramica approfondita delle vulnerabilità critiche che potrebbero essere sfruttate da attaccanti. Questi test rivelano punti deboli nei sistemi, nelle reti e nelle applicazioni, consentendo all'organizzazione di correggerli prima che vengano sfruttati. I risultati devono essere analizzati con attenzione e devono portare a un miglioramento delle difese tecnologiche e operative.

12. Gestione del Rischio dei Fornitori di Servizi ICT

La gestione del rischio dei fornitori di servizi ICT è essenziale per proteggere la resilienza operativa digitale di un'organizzazione. Poiché molte aziende dipendono da terze parti per la fornitura di soluzioni tecnologiche e servizi critici, è fondamentale gestire adeguatamente i rischi associati a questi fornitori. Questo include la valutazione e il monitoraggio dei fornitori, la gestione dei contratti e la definizione di approcci al rischio che coinvolgano i partner esterni. Le linee guida in questa sezione forniscono un quadro per garantire che i fornitori di servizi ICT contribuiscano alla continuità operativa e alla sicurezza delle operazioni aziendali.

12.1 Registro delle Informazioni

Un registro delle informazioni sui fornitori di servizi ICT deve essere mantenuto per garantire che tutte le informazioni relative ai fornitori siano accessibili e aggiornate. Questo registro deve includere dettagli sui contratti, i servizi offerti, i livelli di rischio associati, le misure di sicurezza adottate e i contatti di emergenza. La registrazione accurata delle informazioni permette una gestione efficace e trasparente delle relazioni con i fornitori.

12.2 Approccio al Rischio

L'approccio al rischio dei fornitori di servizi ICT implica la valutazione continua dei rischi associati a ciascun fornitore. L'organizzazione deve definire un processo sistematico per identificare, analizzare e mitigare i rischi provenienti dai fornitori, come vulnerabilità di sicurezza, interruzioni dei servizi, o problemi legali. L'approccio deve anche prevedere l'integrazione del rischio dei fornitori nel più ampio framework di gestione del rischio dell'organizzazione.

12.3 Ruolo di Gestione del Rischio di Fornitori Terzi di Servizi ICT

La gestione del rischio dei fornitori di servizi ICT deve essere responsabilità di un team dedicato, che si occupi della supervisione continua e dell'audit delle prestazioni dei fornitori. Questo team deve essere in grado di monitorare i rischi associati ai fornitori, coordinare le azioni correttive in caso di incidenti, e garantire che i fornitori rispettino gli accordi in termini di sicurezza e continuità dei servizi.

12.4 Valutazione delle Terze Parti

Le terze parti devono essere regolarmente valutate per determinare la loro capacità di fornire servizi sicuri e resilienti. La valutazione include la verifica della loro sicurezza informatica, la solidità finanziaria, la capacità di supportare i requisiti aziendali e la conformità alle normative. I risultati della valutazione devono essere utilizzati per selezionare i fornitori e per determinare la frequenza e l'intensità del monitoraggio.

12.5 Canale di Comunicazione Interno

Un canale di comunicazione interno deve essere stabilito per garantire che tutte le informazioni sui fornitori di servizi ICT vengano condivise tempestivamente tra le funzioni aziendali coinvolte nella gestione del rischio e nella continuità operativa. Questo canale deve facilitare la collaborazione tra i team IT, legale, acquisti e sicurezza, per garantire che le problematiche relative ai fornitori vengano affrontate in modo rapido ed efficace.

12.6 Servizi ICT a Supporto di Funzioni Critiche o Importanti

Quando un'azienda si affida a fornitori di servizi ICT per gestire funzioni critiche o importanti, è fondamentale assicurarsi che questi servizi siano costantemente monitorati e analizzati per prevenire eventuali rischi. La gestione efficace di questi fornitori permette di garantire la continuità operativa e la sicurezza aziendale.

12.6.1 Identificazione dei Servizi Critici

È necessario condurre una mappatura dettagliata dei servizi ICT utilizzati per individuare quelli che, se compromessi, potrebbero avere un impatto significativo sulle attività aziendali. Classificare i servizi in base alla loro importanza consente di stabilire priorità nelle attività di monitoraggio e gestione del rischio. Un'analisi preventiva aiuta a definire misure di sicurezza adeguate per ciascun servizio critico, riducendo così la possibilità di interruzioni operative. Le aziende dovrebbero mantenere un inventario aggiornato di tutti i servizi ICT critici e dei fornitori associati per avere una visione chiara dell'ecosistema digitale aziendale e prevenire possibili vulnerabilità.

12.6.2 Analisi e Valutazione dei Rischi

Ogni fornitore deve essere sottoposto a una valutazione approfondita, prendendo in considerazione l’infrastruttura utilizzata, le misure di sicurezza adottate e la capacità di rispondere prontamente a eventuali incidenti. L'analisi dei rischi deve includere scenari di vulnerabilità, possibili impatti sulle operazioni aziendali e strategie di mitigazione. La conduzione periodica di test consente di simulare situazioni di crisi e verificare la resilienza dei sistemi e la capacità di risposta dei fornitori. Inoltre, l'adozione di strumenti di analisi dei rischi basati su intelligenza artificiale aiuta a identificare tempestivamente eventuali minacce emergenti, aumentando così la sicurezza complessiva dell’azienda.

12.7 Gestione dei Contratti

La gestione efficace dei contratti con i fornitori di servizi ICT è essenziale per garantire sicurezza, continuità operativa e affidabilità dei servizi. Un contratto ben strutturato aiuta a prevenire problematiche legate alla sicurezza e a mantenere un elevato standard di qualità nelle prestazioni dei fornitori.

12.7.1 Definizione Chiara delle Responsabilità

Per evitare incomprensioni e mancanze operative, i contratti devono specificare in modo dettagliato i ruoli e le responsabilità di ogni parte coinvolta. Una chiara definizione delle competenze riduce il rischio di disguidi e assicura che ogni attore conosca esattamente il proprio ambito di intervento. È utile inserire un piano di escalation per la risoluzione delle controversie, così da gestire eventuali problematiche in modo strutturato e tempestivo. Inoltre, un documento di responsabilità condivisa può delineare in modo dettagliato le aree di competenza di ciascun soggetto coinvolto nel contratto, facilitando una collaborazione più efficace e trasparente.

12.7.2 Requisiti Contrattuali

I contratti stipulati con i fornitori di servizi ICT devono prevedere garanzie specifiche per assicurare la continuità del servizio e la protezione dei dati aziendali. È necessario definire clausole che stabiliscano strategie efficaci per mitigare i rischi, procedure dettagliate per la gestione degli incidenti con tempistiche chiare e responsabilità ben definite, nonché tempi garantiti per il ripristino dei servizi in caso di disastro. La protezione e la sicurezza dei dati devono essere elementi centrali degli accordi, con particolare attenzione alla conformità normativa e all'adozione di adeguati standard di sicurezza. È inoltre fondamentale concordare questi aspetti preventivamente e verificarne regolarmente l'applicazione. L'inserimento di penali contrattuali in caso di mancato rispetto degli SLA aiuta a garantire l'adempimento degli impegni presi dai fornitori, mentre la predisposizione di clausole di exit strategy facilita un'eventuale transizione senza problemi in caso di cambio di fornitore.

12.7.3 Sicurezza e Protezione dei Dati

Nel contesto contrattuale, è fondamentale includere clausole precise sulla protezione dei dati aziendali, sul rispetto delle normative vigenti come il GDPR e sulla gestione delle informazioni sensibili. Devono essere stabiliti protocolli chiari di risposta in caso di violazioni della sicurezza, garantendo che eventuali incidenti vengano gestiti con tempestività ed efficienza. L'implementazione di sistemi di crittografia avanzata e l'adozione di meccanismi di accesso controllato ai dati aziendali rappresentano misure essenziali per prevenire fughe di informazioni riservate. Inoltre, è opportuno prevedere l'obbligo contrattuale di notificare tempestivamente qualsiasi violazione dei dati, in modo da attivare immediatamente le procedure di mitigazione necessarie.

12.7.4 Piani di Continuità e Gestione degli Incidenti

Ogni contratto deve prevedere strategie efficaci per garantire la continuità del servizio anche in caso di emergenze, con procedure chiare per la gestione degli incidenti informatici e meccanismi rapidi per la risoluzione dei problemi. La predisposizione di team di risposta agli incidenti con ruoli e competenze specifiche è fondamentale per affrontare tempestivamente eventuali situazioni di crisi. Collaborare con enti governativi e autorità di sicurezza può rappresentare un ulteriore vantaggio nella gestione delle emergenze, consentendo di adottare soluzioni in linea con le migliori pratiche del settore.

13. Conclusione

L'adozione di un solido sistema di gestione del rischio dei fornitori di servizi ICT è cruciale per garantire la resilienza digitale e la continuità delle operazioni aziendali. Le aziende devono monitorare costantemente i propri fornitori, gestire i contratti in modo strategico e avere processi chiari per affrontare le problematiche di sicurezza e continuità. Solo attraverso una gestione attenta dei fornitori è possibile ridurre i rischi e proteggere l'organizzazione da interruzioni non previste.

Impegno dell'Organo di Gestione: Audit Interno

L'organo di gestione deve essere direttamente coinvolto nel monitoraggio e nella revisione dei rischi legati ai fornitori di servizi ICT. Un audit interno regolare, condotto da una funzione indipendente, è essenziale per valutare l'efficacia delle pratiche di gestione del rischio dei fornitori e per garantire che l'azienda rispetti gli standard di resilienza digitale stabiliti. Questo audit deve essere accompagnato da rapporti periodici per fornire una visione chiara della gestione dei rischi e delle azioni correttive adottate.

Attività Previste

Di seguito sono descritte le principali attività che compongono il servizio di consulenza. Ogni fase è progettata per essere modulare e adattabile, con tempistiche e modalità di intervento definite in base alle caratteristiche dell'organizzazione cliente.

Valutazione Iniziale e Analisi del Contesto

- Identificazione e mappatura dei processi critici aziendali che dipendono da sistemi ICT.
- Rilevazione delle infrastrutture tecnologiche esistenti e dei flussi informativi.
- Analisi delle vulnerabilità e delle lacune rispetto ai requisiti DORA.
- Redazione di un report diagnostico che evidenzia le aree di miglioramento e le azioni prioritarie.
- Definizione dei responsabili interni coinvolti nel processo di conformità.

Tempistiche: da 2 a 4 settimane, in base alla complessità dell'organizzazione, subordinatamente alla collaborazione del cliente e dei referenti interni, la cui partecipazione è essenziale per garantirne il buon esito.

Gestione e Valutazione dei Rischi ICT

- Identificazione dei rischi operativi connessi all'uso delle tecnologie digitali.
- Creazione e aggiornamento del registro dei rischi ICT.
- Elaborazione di piani di mitigazione e implementazione delle misure correttive.
- Definizione delle procedure di monitoraggio e revisione periodica dei rischi (almeno annuale).
- Nomina di un responsabile interno per la gestione dei rischi ICT.

Tempistiche: 3 settimane per la valutazione iniziale, subordinatamente alla collaborazione del cliente e dei referenti interni, la cui partecipazione è essenziale per garantirne il buon esito; aggiornamenti annuali o in caso di cambiamenti significativi.

Gestione degli Incidenti ICT

- Redazione di piani di gestione degli incidenti che includono modalità di rilevamento, risposta e recupero.
- Sviluppo di modelli di notifica conformi alle tempistiche previste dalla normativa.
- Simulazioni periodiche per testare l'efficacia delle procedure di risposta.
- Identificazione di figure chiave per la gestione degli incidenti e formazione dedicata.

Frequenza delle simulazioni: almeno semestrale, subordinatamente alla collaborazione del cliente e dei referenti interni, la cui partecipazione è essenziale per garantirne il buon esito.

Testing della Resilienza Operativa

- Programmazione ed esecuzione di test di resilienza (stress test e penetration test) per valutare la capacità di risposta dell'organizzazione a eventi avversi.
- Redazione di report dettagliati con indicazioni sulle azioni correttive necessarie.
- Monitoraggio dei risultati e aggiornamento delle misure di mitigazione.

Frequenza consigliata: annuale, con ulteriori test in caso di modifiche rilevanti alle infrastrutture ICT, subordinatamente alla collaborazione del cliente e dei referenti interni, la cui partecipazione è essenziale per garantirne il buon esito.

Gestione della Catena di Fornitura ICT

- Analisi dei contratti con fornitori terzi e verifica della loro conformità ai requisiti DORA.
- Esecuzione di audit sui fornitori considerati critici per garantire la continuità operativa.
- Definizione di clausole contrattuali per la gestione dei rischi e degli incidenti.

Aggiornamento delle valutazioni dei fornitori almeno una volta l'anno o a seguito di modifiche contrattuali.

Formazione e Sensibilizzazione del Personale

- Erogazione di corsi formativi mirati per i dipendenti e per il management.
- Diffusione di materiali informativi e aggiornamenti normativi.
- Pianificazione di sessioni periodiche di sensibilizzazione per mantenere alto il livello di consapevolezza.

Frequenza: formazione iniziale e aggiornamenti annuali o in caso di modifiche normative.

Monitoraggio Continuo e Aggiornamento delle Procedure

- Verifiche periodiche delle procedure implementate per garantire la conformità costante.
- Reporting mensile o trimestrale sull'avanzamento delle attività e sulle criticità rilevate.

Supporto continuo per l'adeguamento a eventuali aggiornamenti normativi.

Tempistiche previste

Edisoft Srl si impegna con professionalità e puntualità a rispettare le tempistiche pattuite per l'implementazione del progetto, adattandole alle specifiche esigenze del cliente e alle dimensioni della sua organizzazione. L'azienda comprende l'importanza di una pianificazione adeguata e di una gestione accurata per garantire che tutte le fasi del progetto vengano completate nei tempi previsti, in conformità con gli standard di qualità richiesti.

Tuttavia, è **fondamentale sottolineare che la collaborazione dei referenti interni del cliente gioca un ruolo cruciale nel successo del progetto**. La disponibilità e il coinvolgimento attivo dei responsabili aziendali durante l'intero processo sono determinanti per affrontare eventuali problematiche, prendere decisioni tempestive e risolvere situazioni in corso d'opera.

In particolare, per garantire una gestione efficace delle attività relative al protocollo DORA, è essenziale un flusso continuo di informazioni e un supporto concreto da parte del team interno del cliente. Solo attraverso una stretta collaborazione tra il nostro team di consulenti e i referenti aziendali, è possibile assicurare il rispetto delle tempistiche e la completa conformità alle normative, con la massima efficienza e precisione.

Documentazione per la Conformità al Protocollo DORA

Per garantire la conformità al DORA, le organizzazioni devono predisporre un insieme di documenti specifici che attestino l'adozione delle misure richieste dalla normativa. Edisoft Srl assiste i propri clienti nella redazione di tutta la documentazione necessaria, assicurando la conformità ai requisiti e la coerenza con i processi interni.

Elenco dei Documenti Richiesti

1. Politica di Gestione del Rischio ICT
   Descrive le modalità di identificazione, valutazione, gestione e monitoraggio dei rischi ICT.
2. Registro dei Rischi
   Documento che elenca i rischi ICT identificati, con relative valutazioni, piani di mitigazione e responsabili delle azioni correttive.
3. Piano di Gestione degli Incidenti ICT
   Include le procedure di rilevazione, segnalazione e risposta agli incidenti, oltre alle modalità di comunicazione interna ed esterna.
4. Rapporti di Testing della Resilienza
   Comprende i risultati dei test di penetrazione, degli stress test e dei piani di azione conseguenti.
5. Politica di Gestione delle Terze Parti
   Definisce i criteri per la selezione, la valutazione e il monitoraggio dei fornitori ICT critici.
6. Accordi Contrattuali con i Fornitori
   Contengono clausole specifiche per la gestione del rischio ICT e i requisiti di resilienza operativa.
7. Piani di Continuità Operativa e di Ripristino
   Descrivono le misure da adottare per garantire la continuità dei servizi in caso di interruzioni.
8. Formazione e Sensibilizzazione
   Documentazione che attesta la formazione erogata al personale e la partecipazione ai corsi.
9. Report di Monitoraggio e Aggiornamento
   Report periodici che evidenziano lo stato di conformità e le eventuali azioni correttive intraprese.
10. Documentazione sulla Governance ICT
    Includendo la definizione dei ruoli, delle responsabilità e dei flussi decisionali.
11. Eventuale documentazione redatta per certificazioni affini alla tematica del Protocollo Dora (es. ISO27001)

Modalità di Redazione

I documenti verranno redatti dal team di consulenti Edisoft attraverso le seguenti modalità:

- **Analisi iniziale e raccolta dati:** Incontri con i referenti aziendali per comprendere i processi e raccogliere informazioni necessarie.
- **Redazione personalizzata:** Produzione di documenti adattati alle esigenze dell'organizzazione e conformi ai requisiti normativi.
- **Revisione congiunta:** Condivisione delle bozze con i responsabili interni per raccogliere feedback e apportare le modifiche necessarie.
- **Caricamento su Formalize:** Archiviazione dei documenti sulla piattaforma per garantire tracciabilità, sicurezza e aggiornamenti costanti.
- **Aggiornamenti periodici:** Revisione e aggiornamento della documentazione in base alle evoluzioni normative e ai cambiamenti organizzativi.

Soggetti Interni Coinvolti nella Redazione

Per una corretta redazione e implementazione della documentazione, è essenziale coinvolgere diverse figure aziendali, tra cui:

- **CEO o Direzione Generale:** Definizione delle politiche aziendali e approvazione finale dei documenti.
- **Responsabile ICT:** Fornisce informazioni tecniche sui sistemi e partecipa alla definizione dei piani di continuità e gestione incidenti.
- **Compliance Officer:** Supervisiona la conformità normativa e coordina le attività documentali.
- **Risk Manager:** Collabora alla valutazione dei rischi e alla definizione delle strategie di mitigazione.
- **Responsabile Acquisti:** Coinvolto nella gestione dei contratti con i fornitori ICT e nella revisione delle clausole contrattuali.
- **Responsabile delle Risorse Umane:** Coordina le attività di formazione e sensibilizzazione del personale.
- **Dipendenti e Responsabili di Funzione:** Partecipano attivamente alla raccolta delle informazioni e all'attuazione delle procedure.

Il coinvolgimento di tutte queste figure permette di garantire una copertura completa dei requisiti normativi e la creazione di un sistema di gestione efficace e duraturo.

Conclusioni

Adeguarsi al protocollo DORA non rappresenta solo un obbligo normativo, ma un'opportunità strategica per rafforzare la resilienza operativa e la sicurezza dei propri processi aziendali. In un contesto in cui le minacce informatiche sono sempre più sofisticate e le interconnessioni digitali sempre più complesse, investire nella conformità significa tutelare la continuità del business e la fiducia di clienti, partner e investitori.

Affidarsi a Edisoft significa scegliere un approccio orientato ai risultati, incentrato sulle reali esigenze dell'organizzazione e finalizzato a garantire una conformità duratura e sostenibile nel tempo. Siamo pronti a supportarvi in ogni fase, dall'analisi iniziale fino al mantenimento della conformità, con l'obiettivo di trasformare gli obblighi normativi in un valore aggiunto per la vostra azienda.