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

PIANO ADEGUAMENTO DIRETTIVA NIS 2

LINEE GUIDA VERSO LA CONFORMITÀ ALLA NORMATIVA

Il presente documento delineerà l'approccio, l'ambito di applicazione e le attività necessarie per l'adeguamento alla Direttiva NIS 2, 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 informatica e mitigare le vulnerabilità aziendali.

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

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

Sommario

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

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

Introduzione al progetto di consulenza

La Direttiva NIS2 impone nuovi obblighi in materia di cybersecurity per rafforzare la resilienza delle aziende contro le minacce informatiche. L'adeguamento non è solo una questione di conformità normativa, ma un'opportunità per migliorare la sicurezza e la continuità operativa.

Edisoft Srl offre un servizio di consulenza dedicato, guidando le aziende nell'implementazione di misure efficaci per soddisfare i requisiti della NIS2. Dalla valutazione del rischio alla definizione di strategie di sicurezza informatica, fino alla gestione della disclosure e alla formazione del personale, il nostro team fornisce supporto su misura per ogni realtà aziendale. Affidarsi a Edisoft significa scegliere un partner esperto e competente, capace di trasformare le sfide della compliance in un vantaggio competitivo.

Perché scegliere Edisoft

Affidarsi a Edisoft per l'adeguamento alla Direttiva NIS2 significa contare su un team di esperti in cybersecurity e compliance aziendale, in grado di fornire soluzioni concrete e su misura. Grazie alla nostra esperienza trentennale nel settore IT, supportiamo le aziende nell'implementazione di strategie di sicurezza efficaci, minimizzando i rischi e garantendo la conformità normativa.

Oltre alla consulenza operativa, offriamo percorsi di formazione e training dedicati, affinché il personale interno acquisisca le competenze necessarie per gestire autonomamente gli aspetti chiave della sicurezza informatica. Il nostro obiettivo è creare una cultura aziendale solida in materia di cybersecurity, permettendo alle aziende di affrontare con sicurezza le sfide del panorama digitale.

La nostra offerta in merito alla normativa NIS2

Edisoft supporta le aziende nel percorso di adeguamento alla Direttiva NIS2 con un servizio di consulenza completo e su misura, pensato per garantire conformità normativa, sicurezza informatica avanzata e una maggiore resilienza operativa. La crescente complessità delle minacce cyber e l'evoluzione delle normative impongono un approccio strutturato, che non si limiti alla mera compliance, ma favorisca una cultura aziendale orientata alla sicurezza e alla gestione del rischio.

Il nostro servizio inizia con un'analisi dettagliata del business e un'approfondita valutazione dei gap rispetto ai requisiti della NIS2. Attraverso questa fase, identifichiamo le aree critiche e definiamo un piano di adeguamento personalizzato, con azioni concrete per colmare le lacune esistenti e implementare misure di sicurezza efficaci.

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

L'obiettivo è consentire all'azienda di gestire autonomamente i propri processi di cybersecurity, minimizzando le vulnerabilità e migliorando la capacità di risposta a eventuali incidenti.

Un elemento centrale della nostra offerta è la guida e il supporto nella redazione di tutta la documentazione necessaria per una disclosure completa e conforme alla normativa. Il rispetto degli obblighi normativi in materia di segnalazione e gestione degli incidenti cyber è cruciale per evitare sanzioni e garantire la trasparenza nei confronti delle autorità competenti.

Per rafforzare ulteriormente la capacità di difesa dell'azienda e renderla indipendente nella gestione della sicurezza, offriamo anche sessioni di training specifiche per il personale, erogate dai nostri esperti certificati in cybersecurity. Questo percorso formativo è progettato per trasferire competenze operative e strategiche, consentendo ai team aziendali di comprendere e applicare le best practice di sicurezza informatica. Investire nella formazione interna non solo migliora la protezione dell'azienda, ma riduce il rischio di errori umani e garantisce una gestione più efficace delle minacce.

Grazie alla nostra esperienza trentennale nel settore IT, siamo in grado di guidare le imprese verso un futuro più sicuro e conforme, trasformando la compliance in un vantaggio strategico.

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

Redazione della documentazione tramite Formalize

L’implementazione della normativa NIS2 è un processo articolato che richiede il coinvolgimento di diversi attori aziendali e l’adozione di strumenti specifici per garantire la compliance. Formalize è il software scelto da Edisoft, che supporta le aziende nella gestione e monitoraggio della documentazione relativa alla sicurezza informatica.

L'intero processo di compilazione della documentazione avverrà attraverso il software Formalize, che permetterà di creare e gestire utenze personalizzate con permessi differenti. In questo modo, i referenti interni individuati dal cliente potranno fornire la documentazione richiesta in base all'area operativa di cui sono responsabili. Ogni utente avrà accesso solo alle sezioni di competenza, garantendo sicurezza e tracciabilità nelle operazioni di inserimento e revisione.

Ogni attività all'interno di Formalize può essere impostata come "applicabile/non applicabile" e "implementata/non implementata" in base allo stato di avanzamento, garantendo un monitoraggio preciso della compliance NIS2.

Le seguenti sezioni descrivono le fasi del processo di implementazione della NIS2 attraverso Formalize, evidenziando le attività necessarie e il coinvolgimento dei referenti interni designati dal cliente. La collaborazione con questi referenti è fondamentale per garantire un’efficace attuazione delle misure di sicurezza, e le tempistiche per la redazione della documentazione sono stimate su aziende di medie dimensioni. Tuttavia, possono variare in base alla grandezza dell’azienda e alla cooperazione del personale coinvolto.

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

1. Governance

1.1 Impegno dell'organo di gestione

L'organo di gestione aziendale svolge un ruolo cruciale nell'implementazione del framework NIS2, garantendo che la sicurezza informatica sia una priorità strategica. È fondamentale che il management definisca e/o applichi le politiche di cybersecurity, approvi le risorse necessarie e monitori l'attuazione delle misure di sicurezza.

Definizione delle politiche di sicurezza: L'azienda deve stabilire un quadro normativo interno che delinei le politiche di sicurezza, definendo regole e procedure per la gestione del rischio informatico.
L'analisi dei rischi aziendali rappresenta il primo passo per identificare le priorità di sicurezza.
A seguito dell'analisi dei rischi e alla raccolta dei vari documenti, essi daranno luogo all'elaborazione di un documento ufficiale che raccoglie le linee guida adottate, le metodologie di protezione e le misure di prevenzione. Infine, è essenziale comunicare queste policy a tutto il personale aziendale affinché siano comprese e rispettate.

Allocazione delle risorse: Una gestione efficace della sicurezza informatica richiede l'assegnazione di risorse adeguate, sia in termini di budget che di personale qualificato.
L'azienda deve identificare il budget necessario per la cybersecurity, pianificando gli investimenti in infrastrutture e strumenti di sicurezza. È importante stabilire una roadmap finanziaria per assicurare un'adeguata copertura delle spese a lungo termine. Un ulteriore aspetto fondamentale è la definizione di un piano di formazione per i dipendenti, garantendo che tutti abbiano le competenze necessarie per agire in modo sicuro e responsabile.

Supervisione e monitoraggio: Il monitoraggio delle politiche di sicurezza è cruciale per verificare l'efficacia delle misure adottate e garantire la conformità con la normativa NIS2.
L'azienda deve istituire un comitato dedicato alla sicurezza informatica che si occupi di supervisionare l'attuazione delle policy. Devono essere definite metriche di valutazione per monitorare la compliance aziendale nel tempo e identificare eventuali aree di miglioramento. I consulenti Edisoft forniranno un'analisi periodica dei report di sicurezza per garantire un aggiornamento costante delle strategie di protezione e un monitoraggio delle policy di sicurezza.

Tempistiche previste: Il processo di definizione e approvazione delle politiche di sicurezza richiede generalmente dai 2 ai 3 mesi. Come anticipato nella precedente sezione, il monitoraggio delle policy è un'attività continua e costante nel tempo di cui si occuperanno i consulenti Edisoft, insieme ai referenti interni dell'azienda.

Referenti coinvolti: I principali referenti per la governance della sicurezza informatica includono la direzione aziendale, il responsabile IT e il compliance officer, che lavorano in sinergia per garantire il rispetto delle normative.

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

1.2 Gestione e formazione dei dipendenti

La formazione del personale è un aspetto essenziale per rafforzare la sicurezza informatica e ridurre il rischio di attacchi derivanti da errori umani. Essa è parte integrante di quanto previsto dalla normativa e, in accordo con il cliente, Edisoft si occuperà di effettuare dei momenti di training con i referenti e con tutti coloro che sono coinvolti direttamente nelle attività assoggettate alla normativa NIS2.

Organizzazione di corsi di formazione: Un programma di formazione strutturato aiuta i dipendenti a riconoscere e gestire le minacce informatiche. L'azienda deve pianificare corsi di formazione specifici, calibrati in base ai livelli di rischio aziendale e alle mansioni dei dipendenti. I corsi devono essere periodici e aggiornati in base alle nuove minacce emergenti. Inoltre, è fondamentale identificare i dipendenti con un rischio elevato, come amministratori di sistema e dirigenti, affinché ricevano una formazione più approfondita.

Sensibilizzazione sulle minacce informatiche: Oltre ai corsi di formazione, è essenziale implementare attività di sensibilizzazione per mantenere alta l'attenzione sulla cybersecurity. L'azienda può organizzare simulazioni di attacchi informatici per testare la reazione del personale e individuare eventuali criticità nel protocollo di risposta.

Tempistiche previste: La creazione del piano di formazione richiede circa 2 mesi. L'implementazione della formazione è un processo continuo che deve essere costantemente monitorato e aggiornato. Sarà cura dell'azienda definire un soggetto responsabile della formazione interno in modo da avere un punto di contatto con i consulenti Edisoft. L'erogazione dell'attività di training dovrà essere concordata tra Edisoft e il cliente: le tempistiche potrebbero variare in base alle esigenze operative delle parti.

Referenti coinvolti: I principali referenti includono il dipartimento HR, il responsabile della sicurezza IT e eventuali formatori esterni specializzati in cybersecurity.

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

2. Gestione del rischio di Cybersecurity

2.1 Approccio al Rischio

L'approccio al rischio è fondamentale per comprendere e gestire le minacce legate alla cybersecurity all'interno di un'organizzazione. In particolare, si adotta un approccio che prende in considerazione la natura e la probabilità dei rischi, nonché le loro potenziali implicazioni sul business. L'obiettivo è fornire un quadro chiaro per la valutazione continua dei rischi, permettendo di decidere quali misure adottare in modo proporzionale alla gravità degli stessi.

L'approccio proposto è in linea con le normative NIS2, che richiedono una gestione adattiva e dinamica del rischio, inclusa l'implementazione di processi che rispondano rapidamente a nuove minacce. La tempistica per implementare un approccio al rischio efficace richiede una fase di analisi preliminare, seguita da una revisione periodica. Un referente interno del cliente che dovrà essere coinvolto in questa fase sarà il responsabile della sicurezza informatica, che collaborerà con il team di consulenti per definire e aggiornare le politiche di gestione del rischio.

2.2 Proporzionalità Basata su Rischi, Dimensione, Probabilità e Gravità

La proporzionalità basata su rischi è un principio essenziale nella gestione della cybersecurity, che implica una valutazione in cui la risposta alle minacce è calibrata in base alla probabilità e alla gravità del rischio. A supporto della classificazione dei rischi verranno usate diverse matrici direttamente sul portale Formalize. La NIS2 incoraggia l'adozione di misure di sicurezza che siano commisurate alla natura dell'organizzazione e alla criticità dei suoi sistemi informatici.

2.3 Analisi del Rischio e Sicurezza del Sistema Informatico

L'analisi del rischio e la sicurezza del sistema informatico sono fasi centrali nella protezione dei dati aziendali e dei sistemi operativi. In questo contesto, vengono identificate le vulnerabilità esistenti, i potenziali attacchi e le aree che richiedono interventi. L'obiettivo è progettare un sistema di difesa solido che riduca al minimo le possibilità di successo di attacchi cibernetici. La NIS2 richiede una valutazione completa dei rischi informatici, con la messa in atto di strategie di protezione avanzate.

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

3. Misure CRM (Gestione del Rischio Cyber)

3.1 Gestione degli Incidenti

La gestione degli incidenti è un aspetto cruciale nella difesa contro le minacce informatiche. Quando un incidente si verifica, è fondamentale avere un piano di risposta pronto, che includa procedure per identificare, contenere, e risolvere l'incidente in modo rapido ed efficace. Un sistema di gestione degli incidenti ben definito consente di ridurre al minimo l'impatto sulle operazioni aziendali e di prevenire danni a lungo termine. I referenti per questa attività saranno il responsabile della sicurezza IT e il team di incident response, che dovranno collaborare per creare e testare il piano.

3.2 Continuità Operativa

La continuità operativa è essenziale per garantire che l'organizzazione possa continuare a funzionare anche in caso di incidenti gravi o di attacchi informatici. Un piano di continuità operativa (BCP - Business Continuity Plan) deve essere redatto e testato regolarmente, per garantire che tutte le funzioni aziendali critiche possano essere ripristinate rapidamente in caso di disastro. In ambito NIS2, le organizzazioni devono assicurarsi che le loro operazioni possano proseguire senza interruzioni significative, anche in presenza di eventi avversi. Questo processo richiede tempo per identificare le aree vulnerabili e pianificare soluzioni adeguate.

3.3 Sicurezza della Catena di Approvvigionamento

La sicurezza della catena di approvvigionamento è essenziale per proteggere i sistemi informatici da vulnerabilità che potrebbero derivare dai fornitori, dai partner e dalle terze parti con cui l'organizzazione collabora. È necessario eseguire una valutazione dei rischi associati a ciascun attore nella catena di approvvigionamento, monitorando costantemente le loro pratiche di sicurezza. L'approccio NIS2 sollecita un controllo rigoroso su questi aspetti per evitare che vulnerabilità esterne compromettano la sicurezza interna. Il tempo necessario per implementare una strategia di sicurezza della catena di approvvigionamento dipende dalla quantità di fornitori e dalla loro complessità.

3.4 Valutazione del Rischio del Fornitore

La valutazione del rischio del fornitore è una parte fondamentale nella gestione complessiva della sicurezza aziendale, in particolare quando si considera il rischio derivante da terzi. Questo processo prevede l'analisi delle politiche di sicurezza dei fornitori e l'adozione di misure che possano mitigare eventuali rischi. A seguito dell'implementazione di standard di cybersecurity adeguati, la valutazione deve essere continua, poiché nuovi fornitori o cambiamenti nelle pratiche di quelli esistenti potrebbero comportare nuovi rischi.

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

3.5 Sicurezza nei Sistemi Informatici e di Rete

Garantire la sicurezza dei sistemi informatici e di rete è una delle principali preoccupazioni in un contesto di cybersecurity. Questo implica l'adozione di misure protettive per difendere i sistemi aziendali da attacchi esterni, come il rafforzamento delle reti con firewall, intrusion detection systems (IDS), e altre tecnologie di sicurezza avanzate. La sicurezza deve essere continua e riguardare tutti gli aspetti, dall'infrastruttura hardware ai software applicativi, con il supporto di aggiornamenti e patch regolari

3.6 Strategie e Procedure per Valutare la Compliance

Le strategie e le procedure per valutare la compliance sono cruciali per assicurare che l'organizzazione rispetti tutte le normative e gli standard di sicurezza richiesti, tra cui la NIS2. Questo implica la creazione di una serie di controlli e audit per monitorare l'aderenza alle politiche interne e alle normative esterne. Un programma di compliance deve includere attività di revisione periodica, con valutazioni interne e coinvolgimento di consulenti esterni per garantire che tutte le pratiche siano in linea con le leggi vigenti. Di seguito nel documento è predisposta una sezione dedicata alla tematica di Audit.

3.7 Uso di Crittografia

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.

3.8 Risorse Umane

È essenziale che solo le persone autorizzate abbiano accesso alle risorse sensibili. Questo implica oltre la gestione di processi come l'onboarding e l'offboarding dei dipendenti, la gestione dei privilegi di accesso. In seguito nel documento è stata predisposta una sezione dedicata all'attività di onboarding e offboarding.

Azioni di sicurezza come il controllo dei permessi e la separazione dei compiti sono fondamentali per proteggere i dati aziendali, lo stesso grado di sicurezza verrà garantito tramite la piattaforma Formalize in cui le utenze saranno legate a permessi specifici definite in base all'area di attività del dipendente.

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

Il controllo dell'accesso è essenziale per evitare che individui non autorizzati possano accedere a sistemi informatici sensibili. Questo include l'adozione di soluzioni come l'autenticazione multifattoriale (MFA) e la gestione rigorosa dei privilegi degli utenti.

3.9 Gestione degli Attivi

La gestione degli attivi implica il monitoraggio e la protezione di tutte le risorse informatiche aziendali, tra cui hardware, software e dispositivi mobili. La gestione efficace degli attivi aiuta a ridurre il rischio di vulnerabilità derivanti da dispositivi non sicuri o mal configurati.

3.10 Gestione di Autenticazione

La gestione dell'autenticazione è fondamentale per garantire che solo gli utenti autorizzati possano accedere ai sistemi critici. Questo include l'adozione di politiche di gestione delle credenziali, come la password policy, e la protezione contro attacchi come il brute force.

Tempistiche e Referenti Interni Coinvolti

La tempistica complessiva per l'implementazione della consulenza NIS2 e la gestione dei rischi cibernetici è stimata in un arco di tempo che varia a seconda della complessità e delle dimensioni dell'organizzazione.
I referenti interni principali coinvolti includono:
- Responsabile della sicurezza informatica (per la gestione del rischio e l'analisi dei sistemi).
- Chief Risk Officer (per la valutazione della proporzionalità e la gestione dei rischi).
- Direttore IT (per la supervisione dell'adozione degli standard e dei sistemi informatici).
- Chief Procurement Officer e Responsabile Acquisti (per la valutazione dei fornitori).
- Responsabile della Conformità (per la gestione delle certificazioni e della compliance).
- Responsabile delle Risorse Umane (per la gestione della sicurezza delle persone).
- Responsabile della continuità operativa (per il piano di continuità aziendale).

Questi riferimenti dovrebbero essere coinvolti sin dalle fasi iniziali, con un piano di incontri periodici per monitorare i progressi e garantire che le attività siano in linea con le normative e le esigenze aziendali.

3.11 Valutazione del Rischio dei Fornitori: Valutazioni Coordinate dei Rischi per la Sicurezza

La valutazione del rischio dei fornitori è un aspetto cruciale nella protezione dell'intero ecosistema informatico di un'organizzazione. L'analisi dei fornitori deve essere condotta in modo coordinato, considerando i rischi derivanti dalla relazione con ciascun fornitore e come questi possano influire sulla sicurezza complessiva del sistema. Le aziende devono assicurarsi che i fornitori rispettino gli standard di cybersecurity necessari, evitando che vulnerabilità esterne possano compromettere i loro sistemi. La tempistica per completare questa valutazione dipenderà dal numero e dalla complessità dei fornitori coinvolti, ma si prevede che richieda almeno 3 mesi. Il referente per

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

questa attività sarà il Responsabile Acquisti o simili, che lavorernno in collaborazione con il team di sicurezza IT.

3.12 Valutazione del Rischio dei Fornitori: Uso di Sistemi Europei di Certificazione della Cybersicurezza

In ottemperanza alle direttive NIS2, l'uso di sistemi europei di certificazione della cybersecurity è essenziale per garantire che i fornitori adottino le misure di protezione necessarie. L'adozione di tali certificazioni consente alle organizzazioni di fare affidamento su standard di sicurezza riconosciuti a livello europeo, riducendo il rischio di compromissioni da parte di terzi. Questa sezione prevede una revisione delle certificazioni disponibili e la selezione di quelle più appropriate in base ai rischi associati a ciascun fornitore. Il processo di valutazione può durare dai 2 ai 4 mesi e coinvolgerà il responsabile della conformità e il responsabile della sicurezza informatica, che dovranno valutare la compatibilità delle certificazioni con i requisiti aziendali.

Tempistiche e Referenti Interni Coinvolti

- La tempistica complessiva per l'implementazione della consulenza NIS2 e la gestione dei rischi cibernetici è stimata in un arco di tempo che varia a seconda della complessità e delle dimensioni dell'organizzazione. Un altro aspetto cruciale nella definizione delle tempistiche è il grado di collaborazione che i referenti interni hanno nei confronti del progetto.
- I referenti interni principali coinvolti includono:
    - Responsabile della sicurezza informatica (per la gestione del rischio e l'analisi dei sistemi).
    - Chief Risk Officer (per la valutazione della proporzionalità e la gestione dei rischi).
    - Direttore IT (per la supervisione dell'adozione degli standard e dei sistemi informatici).
    - Chief Procurement Officer e Responsabile Acquisti (per la valutazione dei fornitori).
    - Responsabile della Conformità (per la gestione delle certificazioni e della compliance).

Questi riferimenti dovrebbero essere coinvolti sin dalle fasi iniziali, con un piano di incontri periodici per monitorare i progressi e garantire che le attività siano in linea con le normative e le esigenze aziendali.

4. Obblighi di Segnalazione

Il rispetto degli obblighi di segnalazione riveste un ruolo cruciale all'interno della gestione della sicurezza informatica, in particolare nell'ambito delle normative europee come la Direttiva NIS2. È fondamentale che ogni incidente, evento anomalo o attività che possa compromettere la sicurezza dei sistemi informativi aziendali venga tempestivamente segnalato alle autorità competenti, direttamente tramite il portale dell'ACN. Tale segnalazione non solo risponde a specifici requisiti normativi, ma rappresenta anche un passo fondamentale per garantire una risposta rapida e adeguata agli eventi di rischio, al fine di limitare i potenziali danni a livello operativo e

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

reputazionale. Il processo di segnalazione deve essere conforme alle linee guida stabilite dalle autorità di regolamentazione, con un sistema che consenta l'invio di informazioni in maniera strutturata e puntuale.

5. Registrazione di Azienda

La registrazione dell'azienda presso le autorità competenti (tramite il sito https://www.acn.gov.it/portale/home) è un passo obbligatorio per garantire la piena conformità alle normative di sicurezza informatica stabilite dalla Direttiva NIS2 e deve essere effettuata entro le date prestabilite dall'Autorità Cybersicurezza Nazionale. Questo processo implica la raccolta e l'inserimento delle informazioni aziendali necessarie per registrare l'organizzazione nel registro centrale previsto, comprensivo dei dettagli relativi alle risorse come il numero di dipendenti effettivi e parametri economici finanziari tra cui il fatturato e il totale dell'ultimo bilancio approvato.

La registrazione rappresenta un prerequisito fondamentale per essere soggetti a monitoraggio e per poter attuare le misure di protezione previste dalla normativa. Per effettuare correttamente la registrazione dell'organizzazione sul Portale ACN si dovrà essere in possesso dello SPID di un legale rappresentante. Tale attività di registrazione sarà gestita dal team di compliance e sarà completata in una fase iniziale che richiederà circa un mese. Queste sono le tempistiche tecniche necessarie affinché l'ACN possa valutare se l'azienda è un soggetto NIS o meno rientrante nelle categorie "essenziale" o "importante" (maggiori informazioni: https://www.acn.gov.it/portale/nis/ambito).

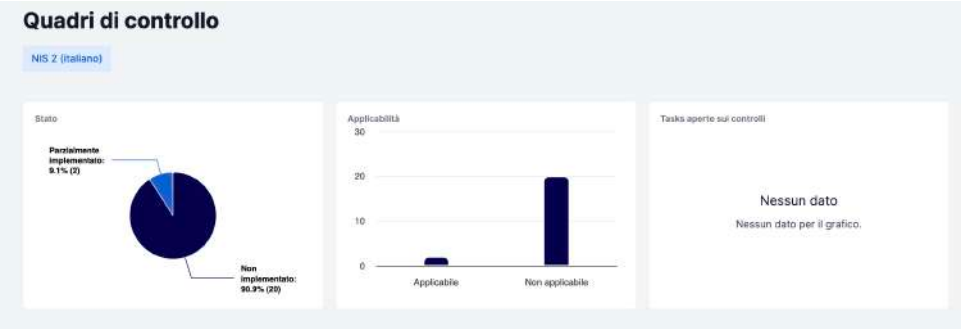
Gestione delle Attività e Task

Le attività progettuali, necessarie per l'attuazione della consulenza NIS2, devono essere suddivise in task specifici e ben definiti. Ogni task avrà una durata prestabilita, assegnando responsabilità chiare agli utenti designati e definendo un livello di priorità in base alla criticità e all'urgenza dell'attività. La suddivisione in task permette una gestione dettagliata e ordinata delle operazioni, facilitando il controllo dei progressi e l'allocazione ottimale delle risorse. Ogni task, che potrebbe riguardare attività tecniche, amministrative o di compliance, sarà monitorato e aggiornato regolarmente. Tempistiche e responsabilità restano tuttavia in capo al personale interno (referenti) dell'azienda che dovranno occuparsi di fornire, entro le scadenze previste, la documentazione necessaria.

Quadri di Controllo e Reportistica

I quadri di controllo presenti sul portale Formalize consentiranno di visualizzare i progressi del progetto attraverso grafici interattivi e report dettagliati, che possono essere esportati in formato Excel per una successiva analisi approfondita. I quadri di controllo non solo offrono una panoramica delle performance in tempo reale, ma permettono anche di identificare eventuali scostamenti rispetto agli obiettivi prefissati, in modo tempestivo e accurato.

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



Identificazione dei Rischi

L'identificazione dei rischi è una fase fondamentale nel processo di gestione della sicurezza informatica, che consiste nel calcolare la probabilità di avvenimento e l'impatto di ciascun rischio. I rischi identificati verranno poi classificati in una heatmap, uno strumento visivo che permette di rappresentare il grado di rischio in base alla combinazione di probabilità e impatto. L'utilizzo di questa mappa consente di attribuire priorità ai rischi più critici e di concentrarsi sugli eventi che potrebbero avere conseguenze più gravi per l'organizzazione.

Grazie al supporto dei referenti interni, i rischi verranno suddivisi in varie sezioni tra cui operativi, legali e informativi. Saranno inoltre, in base alle attività di mitigazione poste in essere, classificati anche in residui, inerenti e potenziali. Ad ogni rischio verrà associato un grado di importanza (basso, medio, alto, critico) e probabilità di accadimento in modo da avere una panoramica esaustiva in continua evoluzione. A seguito delle attività di mitigazione, dovranno essere modificati gli input della heatmap nell'apposita sezione su Formalize.

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

Gestione degli Incidents e Documentazione

La gestione degli incidents è un processo continuo e dinamico che consente di rispondere prontamente a qualsiasi minaccia informatica che possa compromettere la sicurezza aziendale. Ogni incident dovrà essere documentato in dettaglio, raccogliendo tutte le informazioni relative alle cause, alle azioni intraprese e agli esiti dell'incidente stesso. La documentazione sarà fondamentale non solo per la gestione immediata delle situazioni critiche, ma anche per l'analisi post-incidente, al fine di apprendere dall'evento e migliorare le procedure di sicurezza. La gestione degli incidenti avverrà attraverso una sezione dedicata sul portale Formalize, che permetterà la generazione automatica di report e la registrazione delle informazioni chiave.

Risorse

Le risorse, organizzate in modo strutturato e continuamente aggiornato, sono fondamentali per assicurare una gestione ottimale e un controllo accurato delle operazioni aziendali. Di seguito sono elencate le principali risorse che devono essere monitorate e gestite:

- Asset: Insieme delle risorse fisiche e virtuali che supportano le operazioni aziendali, inclusi hardware, software, dati e infrastrutture tecnologiche.
- Dipendenti: Personale che opera all'interno dell'azienda, inclusi ruoli, competenze, accessi e responsabilità all'interno dei sistemi e dei processi aziendali.
- Fornitori: Partner esterni e fornitori di beni e servizi essenziali, che devono essere monitorati per garantire la sicurezza della catena di approvvigionamento e la protezione dei dati.
- Sistemi: Piattaforme tecnologiche, applicazioni software, database e sistemi operativi che gestiscono le informazioni aziendali, critici per il funzionamento e la sicurezza delle operazioni.
- Clienti: Rete di clienti e contatti che interagiscono con l'azienda, il cui trattamento e protezione dei dati sono essenziali per la compliance alle normative di privacy e sicurezza.
- Processi: Procedure aziendali che regolano le operazioni quotidiane, inclusi i processi critici per il business e le funzioni interne.
- Funzioni Aziendali: Aree funzionali come IT, Risorse Umane, Finance, Marketing e altre, che sono parte integrante della gestione delle risorse aziendali e dei flussi di lavoro.
- Contratti: Accordi legali con clienti, fornitori e partner, che definiscono i diritti e gli obblighi in termini di risorse, sicurezza e continuità operativa.
- Flussi di Lavoro: Insieme dei processi aziendali che regolano l'utilizzo delle risorse e garantiscono il raggiungimento degli obiettivi aziendali in modo efficiente e sicuro.

La fase di implementazione di questa sezione richiederà circa 3 mesi, con l'integrazione delle risorse aziendali nel sistema e il continuo aggiornamento delle informazioni critiche.

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

Approccio utilizzato

L'approccio di Edisoft all'adeguamento alla Direttiva NIS2 si fonda su un modello solido e flessibile, progettato per rispondere in modo completo alle esigenze aziendali, adattandosi alle peculiarità di ciascuna realtà. La nostra strategia prevede la creazione di un Modello NIS2, che funge da framework principale per la gestione della sicurezza informatica e per garantire la compliance normativa. Questo modello viene poi personalizzato in base alle specificità di ogni azienda, assicurando un adeguamento preciso, efficace e sostenibile.

Le principali attività del progetto includono l'analisi dei rischi, la definizione delle policy di cybersecurity e la redazione della documentazione strategica, come:

- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Piano integrato per il Risk Management (RM) e la Gestione di Situazioni di Crisi (CM)
- Supply Chain Management (SCM)

Edisoft sviluppa queste attività con un team di esperti in cybersecurity e compliance, definendo inizialmente un modello centrale che, successivamente, viene adattato alle esigenze operative di ciascuna azienda.

Ottica di continuità di business

Il nostro approccio si distingue per l'attenzione alla personalizzazione e all'integrazione. L'obiettivo non è solo implementare un sistema di compliance, ma fare in modo che la sicurezza informatica diventi parte integrante della strategia aziendale, contribuendo a migliorare la resilienza e a garantire la continuità operativa. Ciò significa che lavoriamo per creare soluzioni che siano non solo in linea con la normativa NIS2, ma anche perfettamente allineate alle dinamiche interne e agli obiettivi di business delle aziende con cui collaboriamo.

Inoltre, ci impegniamo a creare un percorso di crescita continua. Non si tratta solo di adeguarsi a una normativa, ma di sviluppare un framework di sicurezza che possa evolvere con l'azienda, grazie a un monitoraggio continuo e a una formazione costante per il personale, in modo da adattarsi alle sfide future in un panorama sempre più complesso e dinamico.

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

Attività del progetto

Il progetto NIS sarà gestito in modo organizzato, garantendo un approccio comune per tutte le attività previste, anche quando la specializzazione su diverse aziende richiederà la personalizzazione in base alla loro dimensione e complessità. Le attività principali del progetto sono le seguenti:

1. Costituzione del Gruppo di Lavoro
   La prima fase consiste nella creazione di un gruppo di lavoro, che includerà una figura di contatto per il progetto NIS e, se necessario, dei sottogruppi tematici per diverse aree, in base alla complessità e alla dimensione della struttura aziendale.
2. Presentazione del Progetto
   Il progetto sarà presentato a tutti i referenti e, quando necessario, ai rappresentanti dei vari gruppi di lavoro. Questo incontro iniziale servirà a definire obiettivi, ruoli e tempistiche, assicurando che tutti i partecipanti abbiano una visione chiara delle fasi successive.
3. Descrizione del Modello Core e Pianificazione delle Interviste
   Ogni area tematica sarà approfondita attraverso degli incontri, durante i quali il modello centrale NIS verrà descritto in dettaglio. In questa fase, si pianificheranno le interviste per raccogliere informazioni cruciali e per comprendere le specifiche esigenze di ciascuna area.
4. Raccolta Dati e Analisi Documentale
   Verranno condotte interviste con i diversi gruppi di lavoro per raccogliere la documentazione applicabile, comprendere i processi aziendali e definire i requisiti specifici di ciascun ambito. Questo processo assicurerà che tutti gli aspetti legati alla sicurezza e alla compliance siano affrontati in modo approfondito.
5. Redazione e Condivisione della Bozza di Documenti
   Una volta raccolti i requisiti, verrà elaborata una bozza dei documenti del modello adattato, che sarà condivisa con il gruppo di lavoro specifico per il feedback e la revisione. Questo passaggio garantirà che ogni documento rispecchi accuratamente le esigenze aziendali e rispetti le normative previste.
6. Finalizzazione e Consegna dei Documenti
   Dopo la revisione, i documenti e i deliverable finali verranno definiti e perfezionati. Sarà assicurata la conformità a tutte le normative NIS2, con la consegna di tutti i documenti chiave per il corretto adeguamento dell'azienda.
7. Supporto sul Campo: Test di Continuità e Allineamento
   I nostri consulenti ed esperti in cybersecurity saranno presenti in azienda durante i test di continuità. Questa fase rappresenterà un'opportunità per condividere e allineare le politiche e le procedure aziendali in merito alla sicurezza, garantendo un'implementazione pratica delle strategie di continuità operativa.

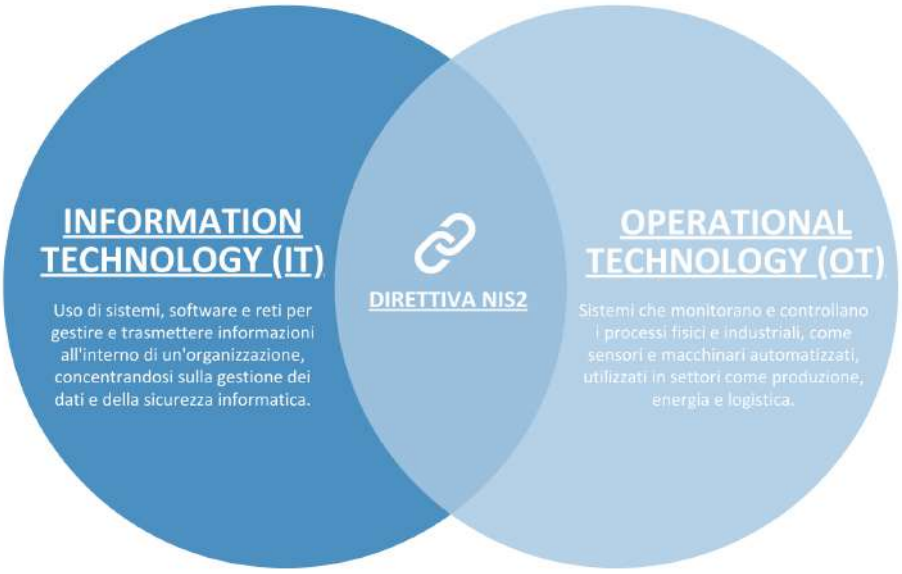
Questo approccio garantisce un processo strutturato e condiviso, in cui ogni passaggio è pensato per coinvolgere attivamente tutte le risorse aziendali, promuovendo la crescita e la resilienza attraverso l'allineamento con le migliori pratiche di sicurezza informatica e la compliance alle normative NIS2.

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

Ambito di applicazione

Il progetto NIS2 si focalizza sull'adozione di misure tecniche, operative e organizzative appropriate e proporzionate, necessarie per gestire in modo efficace i rischi di sicurezza associati ai sistemi informativi e alle reti aziendali all'interno del perimetro operativo. Queste misure saranno progettate per prevenire, ridurre al minimo e gestire l'impatto degli incidenti di sicurezza, garantendo la protezione non solo per gli utenti diretti dei servizi, ma anche per gli altri sistemi e servizi interconnessi.

Un aspetto fondamentale dell'ambito di applicazione riguarda il connubio tra Information Technology (IT) e Operational Technology (OT). Nella visione complessiva del progetto, IT e OT saranno trattati come un tutt'uno integrato, dove le soluzioni di sicurezza dovranno essere applicate in modo coerente a entrambe le dimensioni. La convergenza tra questi due ambiti, che in passato erano separati, impone un approccio unificato per garantire la resilienza operativa digitale. In particolare, la sicurezza delle infrastrutture IT, che gestisce i dati e i sistemi aziendali, deve essere complementare a quella delle tecnologie OT, che si occupano del controllo e della gestione dei processi industriali e operativi.



L'obiettivo è assicurare una protezione completa delle operazioni aziendali, riducendo al minimo i rischi derivanti da vulnerabilità comuni tra i due ambiti e garantendo la continuità e la sicurezza delle operazioni critiche, sia sul fronte digitale che su quello operativo. La gestione integrata della sicurezza tra IT e OT, quindi, rappresenta un elemento centrale per ottenere una resilienza operativa duratura e un'efficace protezione contro le minacce in evoluzione nel panorama della cyber security.

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

Sistema di governance

Edisoft affianca il management aziendale nella definizione e nell'implementazione di un Modello di Gestione per l'adeguamento alla Direttiva NIS2, adottando un approccio strutturato, scalabile e in linea con i principali framework di compliance già consolidati, come GDPR e D.lgs. 231/01. Questo modello rappresenta l'infrastruttura di governance attraverso cui le aziende possono gestire in modo efficace i requisiti normativi, garantendo un livello elevato di sicurezza e resilienza operativa.

Il Modello di Governance ha una duplice funzione: da un lato, fornisce un quadro chiaro e strutturato per la gestione della sicurezza informatica e operativa durante la fase di implementazione del progetto; dall'altro, assicura il mantenimento della compliance nel lungo periodo, attraverso processi di monitoraggio, aggiornamento e miglioramento continuo. Sebbene il modello venga sviluppato nelle prime fasi del progetto, la sua evoluzione è progressiva e viene affinata con il rilascio dei singoli deliverable, assicurando un allineamento costante con le esigenze aziendali e le best practice di settore.

L'output finale è un framework integrato che combina diversi strumenti e metodologie per la gestione del rischio e la protezione delle infrastrutture critiche. Il modello prevede un'analisi approfondita dei rischi ICT e OT, la valutazione dei processi critici attraverso la Business Impact Analysis (BIA) e la definizione di strategie di mitigazione attraverso documenti chiave come il Business Continuity Plan (BCP) e il Disaster Recovery Plan (DRP). Questo approccio consente alle aziende di rafforzare la propria sicurezza informatica e operativa, riducendo i potenziali impatti degli incidenti e garantendo la continuità delle attività.

Elementi chiave del Sistema di Governance

Per garantire un'implementazione efficace e strutturata della NIS2, il Modello di Governance si compone di diversi elementi fondamentali:

- Inquadramento normativo e definizione del perimetro di applicazione
  Viene analizzato il contesto normativo della Direttiva NIS2 e delineato il perimetro aziendale coinvolto, individuando le infrastrutture e i servizi essenziali che rientrano negli obblighi di compliance.
- Struttura organizzativa e ruoli di governance
  Il modello definisce una chiara struttura organizzativa, assegnando ruoli e responsabilità specifiche per la gestione della sicurezza. Sono stabiliti anche i canali di comunicazione interni ed esterni, per garantire un flusso informativo efficiente e reattivo in caso di eventi critici.

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

- Politiche e procedure NIS2
  Vengono sviluppate e implementate politiche di sicurezza conformi alla normativa, che coprono aspetti quali la gestione degli accessi, la protezione delle informazioni, la risposta agli incidenti e la gestione della continuità operativa. Queste policy si applicano su scala globale all'interno dell'azienda e vengono periodicamente aggiornate in base alle evoluzioni normative e tecnologiche.
- Attività di reporting e monitoraggio
  Il sistema di governance prevede una struttura di reporting ben definita, con formati standardizzati e frequenze di aggiornamento precise. Questo consente al management di monitorare costantemente l'efficacia delle misure adottate e di identificare eventuali aree di miglioramento.
- Analisi dei rischi ICT/OT e gestione delle principali procedure di sicurezza
  L'analisi dei rischi copre sia l'ambito IT che quello OT, garantendo un approccio integrato alla sicurezza aziendale. Le principali procedure di sicurezza vengono definite e testate per assicurare la protezione delle infrastrutture critiche e dei processi operativi.
- Documentazione di governance e piano di progetto
  Il modello include tutta la documentazione necessaria per l'adeguamento normativo, tra cui il piano di progetto dettagliato, i protocolli operativi e gli allegati tecnici utili per la gestione e il mantenimento della compliance.

Attraverso questo sistema di governance, Edisoft supporta le aziende nel trasformare l'adeguamento alla NIS2 da un semplice obbligo normativo a un'opportunità per rafforzare la propria sicurezza, migliorare la resilienza operativa e ottimizzare la gestione del rischio in un contesto digitale sempre più complesso.

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

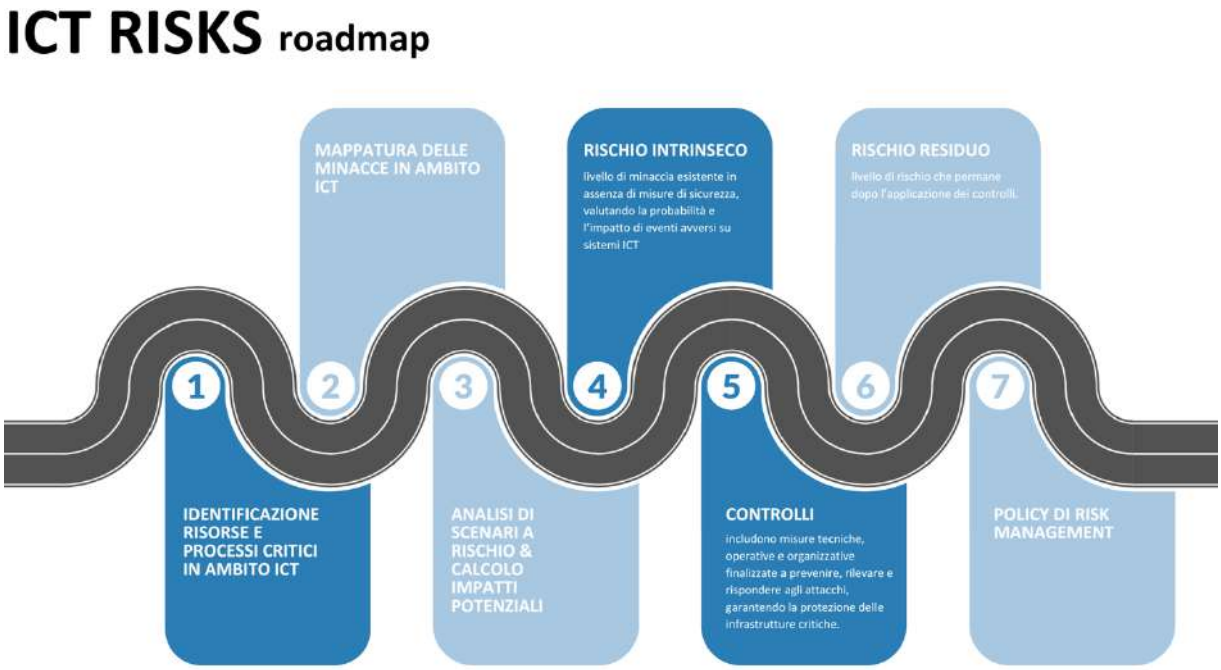
Risk Management

La gestione del rischio è un elemento centrale nell'adeguamento alla Direttiva NIS2, poiché consente di identificare, valutare e mitigare le minacce che possono compromettere la sicurezza e la continuità operativa. Il rischio si suddivide in due ambiti principali: ICT, che riguarda le infrastrutture digitali, i dati e le reti informatiche, e OT, che comprende i sistemi operativi industriali e le tecnologie fisiche che supportano i processi produttivi. Un approccio integrato alla gestione del rischio permette di proteggere entrambi gli ambiti, garantendo la resilienza dell'intera organizzazione.

Rischi ICT

Per garantire la sicurezza dei servizi che supportano i processi critici aziendali, è fondamentale condurre un'analisi dettagliata dei rischi ICT. Questo processo consente di identificare le vulnerabilità dei sistemi digitali, valutare le minacce informatiche e determinare il loro impatto sulle operazioni aziendali.

L'analisi dei rischi ICT si articola in diverse fasi, a partire dalla categorizzazione dei rischi in base alla loro natura e criticità. Viene quindi effettuata una mappatura delle minacce informatiche, con particolare attenzione a scenari di attacco come violazioni dei dati, malware, ransomware e accessi non autorizzati. Infine, attraverso una valutazione dell'impatto, vengono definite le misure di mitigazione e i protocolli di risposta per ridurre il rischio e garantire la continuità operativa. L'adozione di una metodologia strutturata di gestione del rischio ICT consente di implementare controlli efficaci, migliorare la resilienza aziendale e assicurare la conformità con i requisiti della Direttiva NIS2.



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

Rischi OT

Nell'ambito dell'Operational Technology (OT), i rischi non riguardano solo la protezione dei dati, ma anche l'affidabilità, le prestazioni e la sicurezza degli impianti produttivi. I sistemi di controllo industriale (ICS), come PLC, DCS e SCADA, rappresentano il cuore delle infrastrutture operative e necessitano di un'analisi specifica per prevenire potenziali minacce che potrebbero comprometterne il funzionamento.

Per una gestione efficace del rischio OT, adottiamo un approccio basato su standard riconosciuti a livello internazionale, tra cui IEC 62443-3-2, MITRE ATT&CK for ICS, ISO 31010 e NIST 800-82r3. Questo framework consente di identificare vulnerabilità critiche, valutare scenari di attacco e implementare misure di protezione mirate, garantendo così non solo la conformità normativa, ma anche una maggiore resilienza operativa.

Attraverso un'analisi strutturata e un approccio top-down, vengono definiti i livelli di sicurezza target in collaborazione con l'azienda, assicurando un equilibrio tra protezione dei sistemi e continuità produttiva. Le strategie di mitigazione vengono integrate nei processi aziendali, riducendo il rischio di interruzioni e rafforzando la sicurezza complessiva delle infrastrutture industriali.

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

Business Impact Analysis (BIA)

La Business Impact Analysis (BIA) è una componente fondamentale nella valutazione del rischio e nella gestione della continuità operativa. Essa consente di identificare e analizzare i processi aziendali critici, determinando l'impatto che un'interruzione potrebbe avere sull'organizzazione. Il processo di BIA si sviluppa attraverso le seguenti fasi:

1. Customization e Planning: In questa fase, vengono definiti gli obiettivi della BIA, i processi da analizzare e i criteri di valutazione. Viene inoltre pianificata l'organizzazione del progetto e la raccolta delle informazioni necessarie.
2. Interviste & Questionari: Vengono condotte interviste con i principali referenti aziendali per raccogliere dati diretti sulle operazioni quotidiane e sui processi critici. Queste interviste aiutano a comprendere le esigenze specifiche di ogni area dell'organizzazione.
3. Normalizzazione dei Dati: I dati raccolti vengono standardizzati e organizzati per consentire una valutazione uniforme dei processi aziendali. Questa fase garantisce che le informazioni siano pronte per un'analisi comparativa e coerente.
4. Analisi dei Dati: I dati normalizzati vengono analizzati per determinare i potenziali impatti delle interruzioni sui processi aziendali. In questa fase si calcolano i tempi di recupero e le priorità delle azioni da intraprendere.
5. Condivisione dei Risultati: I risultati dell'analisi vengono presentati ai principali stakeholder per ottenere il loro feedback e definire le priorità per il piano di continuità operativa. La condivisione dei risultati è cruciale per allineare il team aziendale sulle misure da adottare.

Deliverables

Nel contesto di progetti complessi come l'adeguamento alla Direttiva NIS2 o altre iniziative di sicurezza informatica e operativa, i deliverables costituiscono la documentazione strategica, i report, le analisi e i piani operativi che consentono di valutare l'efficacia delle misure adottate. Essi sono essenziali non solo per garantire la conformità alle normative, ma anche per migliorare la resilienza e la gestione del rischio aziendale.

I deliverables offerti da Edisoft sono progettati per fornire soluzioni concrete, personalizzate e facilmente implementabili, con un focus particolare sulla trasparenza, l'efficacia e l'allineamento agli obiettivi aziendali.

1. Analisi BIA e Matrice BIA: Un documento che riporta l'analisi dettagliata dell'impatto potenziale delle interruzioni dei processi aziendali, accompagnato da una matrice che classifica la criticità dei processi e dei rischi.
2. Mappatura dei Processi Critici: Una mappatura dei processi aziendali identificati come critici, comprendente le risorse e le dipendenze per garantire la continuità operativa.
3. Identificazione delle Contromisure e del Piano di Rimedio: Una lista di azioni preventive e correttive per mitigare i rischi identificati, insieme a un piano dettagliato per ripristinare la normalità in caso di incidente.

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

Business Continuity Plan

Un Piano di Continuità Aziendale (BCP) ben strutturato è fondamentale per garantire che un'organizzazione possa rispondere efficacemente a situazioni critiche e continuare a operare senza interruzioni significative. Il piano si compone di diverse fasi che permettono di identificare i rischi, implementare strategie di continuità e testare le soluzioni. Di seguito sono illustrate le principali fasi del processo.

1. Identificazione del Contesto e dei Rischi

- **Analisi degli scenari di rischio**: In questa fase vengono esplorati i vari scenari di rischio che potrebbero minacciare le operazioni aziendali, considerando sia eventi esterni (disastri naturali, attacchi informatici) che interni (guasti tecnici, malfunzionamenti).
- **Definizione dei sistemi critici**: Vengono identificati i sistemi, applicazioni e processi essenziali per l'operatività dell'azienda. La mappatura di questi sistemi è cruciale per concentrare gli sforzi di continuità dove sono più necessari.

2. Valutazione dei Rischi e Analisi d'Impatti

- **Analisi dei rischi ICT e OT**: Vengono esaminati i rischi specifici legati sia ai sistemi ICT (Information and Communication Technology) che OT (Operational Technology), per comprendere le vulnerabilità di ciascun ambito.
- **Business Impact Analysis (BIA)**: Si svolge un'analisi approfondita per determinare l'impatto di ciascun rischio sui processi aziendali critici. I risultati della BIA vengono utilizzati per identificare i rischi residui e definire le priorità di intervento.

3. Sviluppo delle Strategie di Continuità

- **Identificazione dei requisiti**: In questa fase si definiscono i requisiti necessari per garantire la continuità dei sistemi IT e OT esistenti. Viene analizzata l'adeguatezza delle tecnologie e delle procedure attuali rispetto ai requisiti individuati.
- **Valutazione della tecnologia e delle procedure**: Si verifica l'efficacia delle soluzioni tecnologiche e delle pratiche organizzative esistenti per assicurarsi che siano in grado di soddisfare le esigenze di continuità operativa.

4. Struttura Organizzativa per la Continuità

- **Definizione del modello organizzativo**: Si sviluppa una struttura organizzativa che include ruoli chiave e responsabilità, come il Comitato Direttivo, il Responsabile della Continuità Operativa, i Responsabili delle Unit e il Team Tecnico.
- **Strategie di attuazione**: Vengono delineate le strategie operative necessarie per garantire il ripristino rapido delle funzioni aziendali critiche, inclusi i processi di gestione delle risorse.

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

5. Creazione del Piano di Continuità Operativa

- Politica di continuità operativa: Si stabilisce una politica di continuità che fissa obiettivi chiari e linee guida per la gestione delle emergenze.
- Piano operativo: Si definisce un piano dettagliato per il recupero delle attività aziendali in caso di interruzione, includendo azioni specifiche e risorse necessarie per il ripristino.
- Metodologia di testing e audit: Vengono definiti i metodi di verifica dell'efficacia del piano tramite simulazioni di scenari di emergenza e audit sui risultati dei test.

6. Validazione e Test del Piano di Continuità

- Individuazione delle carenze: Durante la fase di testing, vengono identificate le lacune nel piano, come procedure inefficienti o tecnologie non adeguate.
- Verifica delle procedure: Si effettuano test operativi per validare le procedure di risposta e per assicurarsi che tutte le fasi del piano possano essere attuate correttamente.
- Formazione del personale: Si organizzano sessioni di formazione per il personale, assicurando che siano pronti ad affrontare le emergenze con conoscenze adeguate.
- Ottimizzazione continua: I risultati dei test e le performance del piano sono utilizzati per apportare miglioramenti continui e garantire che il piano rimanga sempre adeguato e reattivo alle nuove sfide.

Il Piano di Continuità Aziendale è un documento strategico che fornisce all'azienda le linee guida per affrontare le emergenze e garantire che l'organizzazione possa riprendersi velocemente da eventi critici, minimizzando l'impatto sul business. Il piano è un processo dinamico che viene continuamente aggiornato e testato per rimanere efficiente nel tempo.

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

Disaster Recovery & Crisis Management

Disaster Recovery

Il Piano di Disaster Recovery (DRP) è essenziale per garantire la rapida ripresa delle operazioni aziendali in caso di disastri, siano essi tecnici, naturali o di altra natura. Il piano si compone di diverse fasi fondamentali, che vanno dalla definizione di cosa costituisce un "disastro" fino alla gestione post-evento. Di seguito sono delineati gli elementi chiave del processo di Disaster Recovery, le fasi di attuazione e i risultati finali.

1. Definizione del Disastro e Criteri di Attivazione

- **Definizione chiara di "disastro"**: Il piano inizia con una definizione precisa di cosa si intende per disastro, identificando i vari tipi di eventi che potrebbero minacciare la continuità operativa (es. guasti tecnici gravi, attacchi informatici, disastri naturali).
- **Criteri di attivazione**: Vengono stabiliti i criteri specifici che determinano quando il piano di Disaster Recovery deve essere attivato, basandosi sulla gravità dell'incidente e sull'impatto sulle operazioni aziendali.

2. Procedure e Responsabilità

- **Procedure di attivazione**: Si definiscono le procedure dettagliate che devono essere seguite per dichiarare ufficialmente lo stato di emergenza, attivando le fasi del piano. Queste procedure descrivono le azioni necessarie per minimizzare l'impatto e avviare il recupero.
- **Ruoli e responsabilità**: Ogni membro dell'organizzazione coinvolto nel processo di recupero ha ruoli e responsabilità chiaramente delineati. Questo include il responsabile della gestione della crisi, il team di ripristino IT, e le figure di coordinamento interdipartimentali.

3. Gestione della Crisi e Struttura Organizzativa

- **Modalità e protocolli per dichiarare una situazione di crisi**: Vengono descritti i protocolli per la comunicazione interna ed esterna in caso di crisi. Questo include l'allerta delle figure responsabili, la comunicazione con i dipendenti e i clienti, e la gestione delle risorse.
- **Struttura organizzativa**: Si crea una struttura organizzativa dedicata alla gestione del disastro, con un comitato di crisi che supervisiona le attività di recupero e coordina le risorse aziendali. Il comitato è composto da rappresentanti delle diverse aree aziendali critiche.

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

4. Livelli di Servizio e Ripristino

- Livelli di servizio garantiti: Vengono definiti i livelli di servizio minimi da garantire durante la crisi e nelle fasi successive di ripristino. Questo include la disponibilità delle risorse tecnologiche, la continuità di determinati processi aziendali e il recupero dei dati.
- Fase di ripristino: Si stabiliscono le priorità di ripristino, assicurandosi che le operazioni più critiche vengano ripristinate prima e che il ripristino avvenga nel minor tempo possibile, limitando l'impatto sull'operatività complessiva.

5. Ritorno alla Normalità e Strategie di Miglioramento Continuo

- Strategie per il ritorno alla normalità: Una volta gestita la crisi, vengono implementate le condizioni e le strategie necessarie per tornare alla normale operatività aziendale. Questo processo implica il monitoraggio della ripresa e la verifica della piena funzionalità dei sistemi.
- Miglioramento continuo: Dopo ogni attivazione del piano di Disaster Recovery, vengono valutati i risultati e le procedure per identificare eventuali aree di miglioramento. Questo permette di adattare e rafforzare il piano in vista di possibili futuri disastri.

6. Risultati Finali

Il piano di Disaster Recovery si conclude con i seguenti deliverables:

- Criteri e piano di ripristino di emergenza: Documento che stabilisce le priorità di ripristino e le azioni necessarie per il recupero completo delle operazioni aziendali.
- Piano di test del Disaster Recovery: Dettagli delle modalità di test del piano, per garantirne l'efficacia prima e dopo l'attivazione.
- Materiali di formazione per il personale: Documentazione e sessioni formative destinate al personale per familiarizzarsi con le procedure di emergenza e le azioni da intraprendere in caso di disastro.
- Rapporti di audit post-test: Dopo ogni test, vengono redatti rapporti di audit che analizzano i risultati, individuano eventuali lacune nel piano e propongono miglioramenti.

Il Piano di Disaster Recovery rappresenta quindi una parte essenziale della strategia di continuità aziendale, mirato a garantire che l'azienda possa riprendersi rapidamente da eventi critici, mantenendo l'operatività e riducendo al minimo l'impatto negativo.

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

Crisis Management

La gestione delle crisi è un approccio sistematico per affrontare eventi imprevisti che minacciano l'integrità o la continuità delle operazioni aziendali. Un piano ben strutturato e attuato tempestivamente può ridurre significativamente i danni, proteggendo la stabilità e la reputazione dell'organizzazione.

1. Rilevamento e Attivazione della Crisi

- **Monitoraggio continuo e identificazione precoce**: È essenziale che l'azienda implementi un sistema di monitoraggio continuo per identificare segnali precoci di crisi. Ciò include l'osservazione di anomalie nei processi aziendali, sistemi tecnologici, o fattori esterni che potrebbero evolvere in una minaccia significativa.
- **Valutazione dell'impatto e categorizzazione dell'emergenza**: Una volta identificata una potenziale crisi, il passo successivo è determinarne la gravità. Le crisi vengono classificate in base al loro impatto operativo, con categorie che vanno da situazioni minori a emergenze gravi, per indirizzare adeguatamente le risorse e le azioni.
- **Attivazione dei piani di emergenza**: In base alla gravità della crisi, si attivano i piani d'emergenza predefiniti, che stabiliscono azioni immediate per contenere e limitare i danni derivanti dall'incidente.

2. Composizione del Team di Gestione

- **Formazione del team di crisi e assegnazione delle responsabilità**: Un team dedicato alla gestione della crisi viene rapidamente formato, con compiti e responsabilità specifiche assegnate a ciascun membro. La composizione del team dipende dalla natura della crisi e include figure di leadership e competenze tecniche appropriate.
- **Definizione delle linee di comunicazione e escalation**: Le procedure di comunicazione devono essere chiare e rapide, assicurando che le informazioni importanti raggiungano tempestivamente i decisori. Inoltre, viene stabilito un protocollo di escalation che garantisce che le crisi vengano gestite ai livelli più appropriati.
- **Coordinamento con entità esterne**: È fondamentale coordinarsi i partner commerciali e altre parti interessate per gestire la crisi in modo efficace e mantenere la trasparenza. Il coordinamento con attori esterni contribuisce anche a minimizzare i danni reputazionali.

3. Risposta e Recupero

- **Definizione di azioni strategiche di risposta**: Una volta identificata la crisi, il team sviluppa azioni immediate per rispondere alla situazione. Le risposte devono essere tempestive e mirate a ridurre il danno, adattandosi all'evolversi della crisi.
- **Pianificazione di misure correttive e preventive**: Oltre alla risposta immediata, è cruciale identificare azioni correttive per ripristinare la normalità e adottare misure preventive per ridurre la probabilità che la stessa crisi si ripeta in futuro. Ciò include l'adozione di nuove politiche, miglioramenti tecnologici o revisione dei processi aziendali.

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

Supply Chain Management

La gestione dei rischi nella catena di approvvigionamento, in particolare per quanto riguarda gli aspetti legati alla sicurezza informatica e alla conformità alle normative NIS2, è fondamentale per garantire la continuità operativa e la protezione dei dati aziendali. Un approccio strutturato e proattivo è essenziale per minimizzare i rischi derivanti dalla supply chain.

1. Valutazione dei Fornitori Critici

La prima fase consiste nell'effettuare una valutazione approfondita dei fornitori critici che operano nel perimetro NIS2. Questo processo include una revisione completa degli aspetti relativi alla sicurezza dei dati, alla gestione del rischio informatico e alla conformità alle normative di sicurezza pertinenti. È essenziale analizzare se i fornitori rispettano gli standard di sicurezza informatica, le normative locali e internazionali, e se sono in grado di gestire adeguatamente le minacce informatiche.

2. Monitoraggio Continuo

Per proteggere la catena di fornitura da minacce esterne, è fondamentale stabilire un sistema di monitoraggio continuo. Questo sistema deve rilevare anomalie o attività sospette nei processi della supply chain. L'uso di soluzioni di analisi comportamentale può essere utile per identificare pattern anomali, segnalando potenziali vulnerabilità o attacchi in corso.

3. Business Continuity Planning (BCP)

La gestione del rischio nella supply chain deve includere la creazione di piani di continuità aziendale (BCP) specificamente orientati a garantire la resilienza alle interruzioni causate da eventi cibernetici. Tali piani devono considerare scenari di cyber disruption, come attacchi informatici a fornitori o interruzioni dei flussi di dati, e stabilire misure per il ripristino rapido delle operazioni aziendali.

4. Formazione e Sensibilizzazione

È cruciale fornire formazione e sensibilizzazione continua in materia di sicurezza informatica ai dipendenti, concentrandosi in particolare sui rischi legati alla catena di approvvigionamento. I dipendenti devono essere informati sui potenziali attacchi informatici che possono arrivare attraverso i fornitori e sulle pratiche di sicurezza da adottare per proteggere l'integrità dell'azienda.

5. Conformità Normativa e Audit

Infine, è necessario garantire che tutti i fornitori e partner rispettino rigorosamente le normative e gli standard di sicurezza applicabili. Ciò include la verifica periodica della conformità tramite audit regolari, che consentano di monitorare l'efficacia delle misure di sicurezza adottate e di correggere eventuali lacune. Gli audit dovrebbero coprire sia le politiche interne dei fornitori che le misure di sicurezza implementate per proteggere i dati e i sistemi informatici.

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

L'approccio alla gestione dei rischi nella catena di approvvigionamento deve essere continuo, flessibile e in grado di adattarsi alle nuove minacce e alle evoluzioni normative. Un controllo attento e una gestione strategica della supply chain sono elementi chiave per garantire la sicurezza, la resilienza e la conformità alle normative NIS2.

Conclusioni

Il nostro approccio si basa sulla creazione di soluzioni su misura, che tengano conto delle specifiche esigenze operative e dei rischi associati ai diversi settori di business. Siamo in grado di offrire un progetto NIS2 scalabile, che va dalla valutazione preliminare dei rischi fino alla definizione delle politiche di sicurezza, passando per la personalizzazione dei piani di continuità operativa e disaster recovery, in base all'ampiezza e alla complessità delle infrastrutture IT e OT aziendali.

Grazie alla nostra esperienza consolidata nel settore della cyber security, possiamo adattare ogni fase del progetto alla fattispecie specifica di business, garantendo soluzioni efficienti, in grado di rispondere alle normative e di proteggere le risorse critiche dell'azienda. Restiamo a disposizione per ogni chiarimento, pronti a supportarvi nella realizzazione di un piano di adeguamento NIS2 che risponda alle vostre necessità, sia che operiate in un contesto di piccole dimensioni sia in una realtà più strutturata.

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