GRUPPO HERA

Hera_Pro EMPOWER

Insieme, per la crescita dei fornitori

Programma Sviluppo Fornitori *Hera_pro* EMPOWER

GRUPPO HERA

Hera_Pro EMPOWER

Insieme, per la crescita dei fornitori

CONVENZIONE HOWDEN

Servizi ai fornitori

HOWDEN

I servizi proposti

1. Cyber Risk

2. Due Diligence assicurativa

3. Gestione degli appalti

4. Claims Advisory
Perizie di parte

Cyber Risk

Che c'è il Cyber +

Processo semplificato di trasferimento del #1 rischio aziendale percepito

Una proposta assicurativa cyber best in class disponibile nell'arco di poche ore, che include assistenza in caso di sinistro 24/7

Servizi integrati in Cyber +

(senza costi addizionali)

Mappatura

- Analisi della postura di rischio cyber aziendale tramite Cyberwrite. Usiamo la tecnologia per eliminare la necessità del questionario assuntivo.

Semplificazione

- I migliori assicuratori cyber nel mercato, con comprovata esperienza nella sottoscrizione e nella gestione sinistri
- Normativo di polizza revisionato da esperti Howden
- Approccio "On track" che permette a tutti i clienti di ottenere una quotazione assicurativa e servizi di consulting per l'implementazione dei requisiti necessari al miglioramento della stessa

Monitoraggio

- Monitoraggio attivo del rischio tramite Cyberwrite
- Onboarding della polizza e consulenza in ambito sinistri

Parametri

- Aziende fatturato <250mln
- Territorialità: mondo intero esclusa USA

Direttiva Nis 2

Check-up Cyber NIS 2

Le finalità della direttiva:

- migliorare la cooperazione tra gli Stati membri,
- armonizzare le misure di sicurezza cyber,
- responsabilizzare il Top Management, imporre misure di sicurezza agli operatori di servizi essenziali e importanti e le loro supply chain,
- adottare misure di sicurezza adeguate notificare tempestivamente egli incidenti all'Autorità competente ed ai fruitori dei propri servizi.

Gli obblighi generali

- **Governance**

  Il Management dovrà approvare le misure per la gestione dei rischi adottate dall'organizzazione e valutarne l'efficacia nel tempo; seguire una formazione periodica su tematiche di cybersicurezza e offrire una formazione analoga ai dipendenti.

- **Gestione del rischio**

  L'organizzazione dovrà valutare i rischi di sicurezza e di rete e adottare misure tecniche, operative e organizzative adeguate e proporzionate per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei propri servizi

- **Continuità operativa**

  L'organizzazione dovrà adottare soluzioni per garantire la continuità operativa (es. backup, piano di disaster recovery e procedura di gestione delle crisi) finalizzate a ridurre al minimo l'impatto di eventuali interruzioni dei servizi erogati.

- **Supply Chain**

  L'organizzazione dovrà valutare la sicurezza informatica nella catena di approvvigionamento dei prodotti e servizi utilizzati per la fornitura dei propri servizi. La valutazione riguarderà i fornitori ICT e altri fornitori critici che potrebbero causare l'interruzione del servizio per il quale l'organizzazione è stata inclusa nel perimetro NIS2.

I contenuti

Principali misure richieste

- ✓ Politiche di *analisi dei rischi* e di *sicurezza* dei sistemi informativi
- ✓ Procedura di *gestione degli incidenti*
- ✓ Soluzioni per la *continuità operativa* (backup e disaster recovery) e procedure di *gestione e comunicazione* in caso di crisi
- ✓ Politiche di sicurezza della *catena di approvvigionamento* (fornitori e i prestatori di servizi)
- ✓ Sicurezza nell'*acquisizione*, nello *sviluppo*, nella *manutenzione* e nella *gestione* delle *vulnerabilità* dei *sistemi informativi* e delle *reti*
- ✓ Valutazione dell'efficacia della gestione dei rischi di cybersecurity
- ✓ Pratiche di *igiene informatica* di base e *formazione* in materia di cybersecurity
- ✓ Politiche e procedure e di *crittografia e cifratura*
- ✓ Sicurezza delle *risorse umane*
- ✓ Politiche di *controllo degli accessi* e di *gestione degli asset*
- ✓ Uso dell'*autenticazione a più fattori* o di soluzioni di autenticazione continua
- ✓ *Sistemi di comunicazione* vocale, video, di testo e di emergenza protetti

Le misure dovranno essere *proporzionate al contesto ed ai rischi specifici* di ciascun soggetto considerando il grado di esposizione, le dimensioni dell'organizzazione e la probabilità e gravità degli incidenti (come l'impatto sociale ed economico).

Tempistiche

Recepita dall'Italia con il **Dlgs 138 04/09/2024** e con **la Legge 90/2024** (cybersicurezza PA)
Febbraio 2025 - registrazione soggetti interessati su portale ACN
Aprile 2025 - conferma dei soggetti obbligati

9 mesi - periodo transitorio per soddisfare gli obblighi di base (es. notifica incidenti)
18 mesi - periodo transitorio per implementare le misure di sicurezza e raggiungere la compliance

Primi adempimenti

Registrare l'azienda nella piattaforma ACN identificando un punto di contatto dell'ente con il relativo ruolo

Notificare al CSIRT Italia **ogni incidente** con impatto significativo nella fornitura dei servizi; aggiornare l'Autorità con una **relazione intermedia;** stendere una **relazione finale** entro un mese dalla notifica dell'incidente

Sanzioni amministrative

Pecuniarie: in base a gravità dell'evento, danno causato, recidività e cooperazione

Amministrative:
- Obbligo di **rendere pubbliche le violazioni** alla direttiva e/o al Dlgs 138
- Obbligo di **informare il pubblico sugli incidenti** occorsi
- **Interdizione temporanea** degli organi di amministrazione, degli organi direttivi e delle funzioni dirigenziali (AD / rappresentante legale)

Solo per i soggetti essenziali:
- **Sospensione** delle certificazioni e delle **autorizzazioni** per i servizi o le attività forniti
- **Responsabilità diretta** dei **soggetti fisici** degli organi di amministrazione, degli organi direttivi e delle funzioni dirigenziali delle aziende private

Solo per le pubbliche amministrazioni:
- **Responsabilità** dirigenziale, disciplinare e amministrativo-contabile per i **dipendenti pubblici e funzionari** eletti o nominati che esercitano poteri di rappresentanza di un soggetto essenziale (Legge 90/2024)**.**

I contenuti

Criterio settoriale	**Soggetti Essenziali** Grandi operatori di settori essenziali e casi speciali	**Energia** (elettricità, petrolio, gas, calore, idrogeno) | **Sanità** (servizi, laboratori, R&S, prodotti farmaceutici) | **Trasporti** (aerei, ferroviari, idrici, stradali) | *Banche* | *Mercati finanziari* | Imprese e fornitori di **acqua potabile** | Imprese e fornitori di **acque reflue** | **Digitale** (fornitore di: Internet Exchange Points (IXP), fornitori di servizi DNS, registri di nomi TLD, servizi di data center, fornitori di servizi di cloud computing, reti di distribuzione di contenuti, servizi fiduciari) | Gestione dei **servizi ICT**| **Spazio**
	Soggetti Importanti Grandi e medi operatori	**Servizi postali** | **Servizi** di **corriere** | **Gestione** dei **rifiuti** | Produzione e distribuzione di **sostanze chimiche** | Produzione, trasformazione e distribuzione di **alimentari** | **Industria** (dispositivi medici e diagnostici; computer, elettronica e ottica; macchinari/apparecchiature n.c.a.; autoveicoli, rimorchi e altri mezzi) | **Servizi digitali** (mercati online, motori di ricerca online, social network) | **Istituti di Ricerca**
	Pubbliche Amministrazioni Pubbliche amministrazioni centrali, regionali, provinciali ed altri soggetti pubblici	**Amministrazioni centrali** (Organi costituzionali e di rilievo costituzionale, Presidenza del Consiglio dei Ministri e i Ministeri; Agenzie fiscali, Autorità amministrative indipendenti) | **Amministrazioni regionali** (Regioni e Province autonome) | **Amministrazioni locali** (Città metropolitane, Comuni > 100.000 abitanti, Comuni capoluoghi di regione, Aziende sanitarie locali) | **Altri soggetti pubblici** (Enti di regolazione dell'attività economica, Enti produttori di servizi economici, Enti a struttura associativa, Enti produttori di servizi assistenziali, ricreativi e culturali, Enti e Istituzioni di ricerca, Istituti zooprofilattici sperimentali) | **Ulteriori tipologie di soggetti** (Soggetti che forniscono servizi di trasporto pubblico locale, Istituti di istruzione che svolgono attività di ricerca, Soggetti che svolgono attività di interesse culturale, Società in house, Società partecipate e Società a controllo pubblico)
Criterio dimensionale	**Grandi imprese**: più di 250 dipendenti e oltre 43 mln € fatt.	**Medie imprese**: tra 50 e 249 dipendenti e tra 10 e 43 mln € fatt.	**PMI** con ruolo cruciale nel proprio settore, indipendentemente dalle dimensioni
Ruolo delle Autorità	**ACN** (Agenzia per la Cybersicurezza Nazionale) Autorità Nazionale NIS 2 **- Supervisione** proattiva dei Soggetti Essenziali **- Vigilanza** reattiva dei Soggetti Importanti	**CSIRT** (Gruppo nazionale di risposta agli incidenti di sicurezza informatica) **- Gestione incidenti** di sicurezza informatica	

Modalità

Categorie dei fornitori: **soggetti importanti obbligati NIS 2** (es. gestione rifiuti | industrie chimiche | industrie produttive (dispositivi medici e diagnostici; computer, elettronica e ottica; macchinari/apparecchiature n.c.a.; autoveicoli, rimorchi e altri mezzi) e **altri fornitori esposti ai rischi cyber o interessati** a migliorare la sicurezza informatica.

Analisi: **intervista** in video conferenza con il Responsabile IT.

Le misure di sicurezza saranno discusse in base ad un framework specifico, che considera anche gli obblighi NIS 2 e i requisiti del mercato assicurativo.

Gli esiti saranno riassunti in un **report** con suggerimenti e presentati all'Alta Direzione del fornitore.

Output: report con suggerimenti per il fornitore.

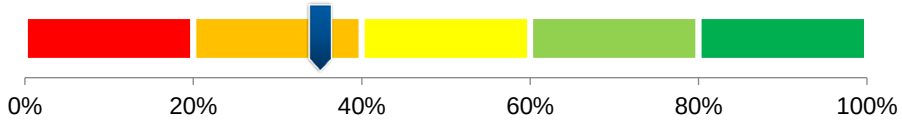
Tempi: predisposizione del report entro 20 giorni dall'intervista

Requisiti di sicurezza e resilienza soddisfatti

	Essenziali	%	Importanti	%	Desiderabili	%	Totale	%
N° requisiti analizzati	10		23		27		60	
Soddisfatti o non applicabili	3	30%	14	61%	11	41%	28	47%
Parzialmente soddisfatti	3	30%	2	9%	6	22%	11	18%
Non soddisfatti o mancanza informazioni	4	40%	7	30%	10	37%	21	35%

Requisiti soddisfatti per area tematica

Livello di compliance NIS 2



Due Diligence Assicurativa

Per ogni polizza analizziamo le seguenti prestazioni:

Rating Compagnia, Impostazione del programma, testo e condizioni, massimali/limiti e premio, a cui sono assegnare specifici “Score” che indicano se le prestazioni sono in linea o meno con i benchmark di mercato.

Dalla media di tali punteggi si potrà ottenere un “Global Score” con l’obiettivo di fornire l’indicazione della qualità complessiva del contratto sottoscritto.

La valutazione è espressa sulla base di una scala numerica che va da 1 a 10, dove 1 indica la non adeguatezza del contratto e 10 l’eccellenza.

Sotto
gli standard di mercato

In linea con
gli standard di mercato/Migliorabile

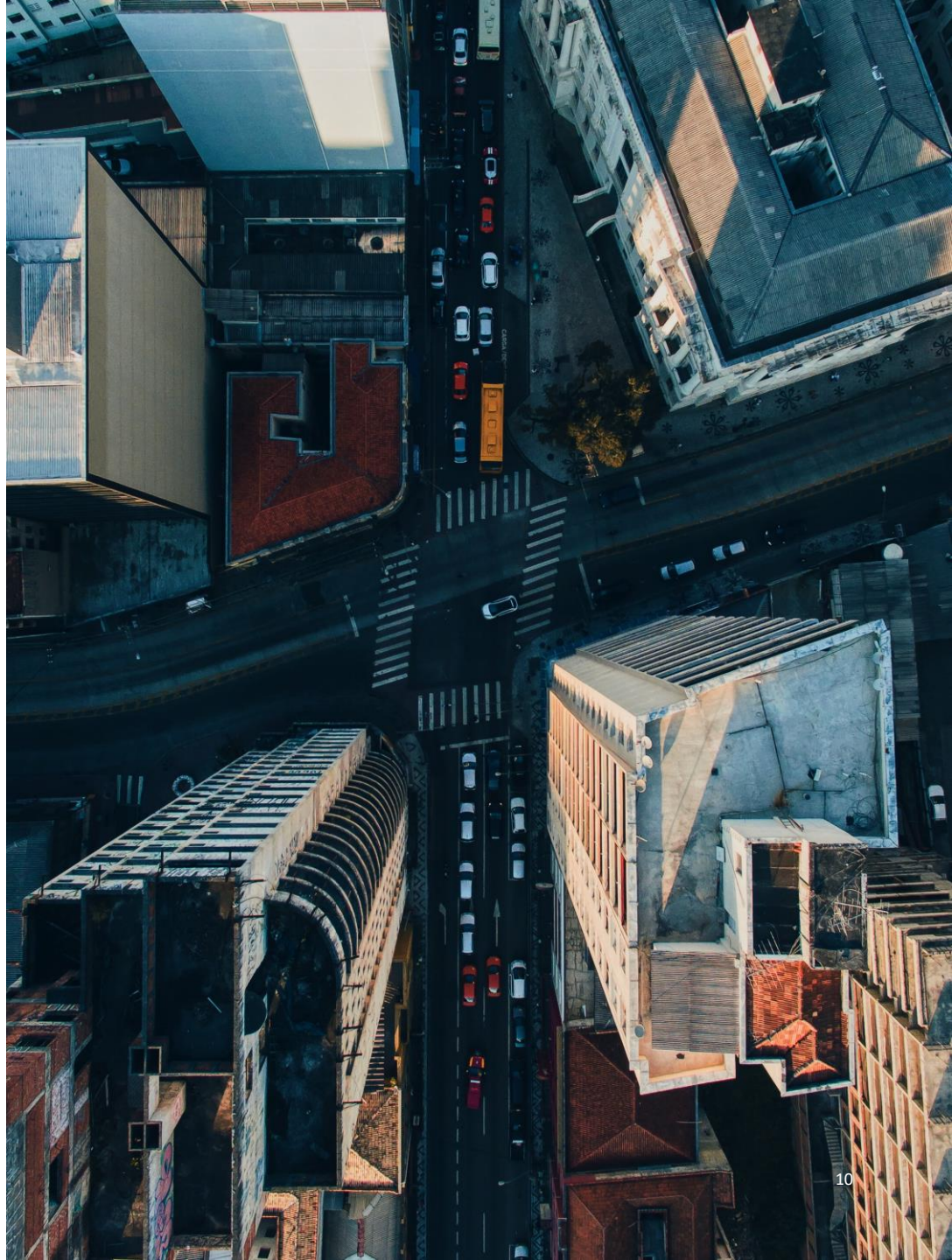
Sopra
gli standard di mercato

Gestione assicurativa degli appalti

Supporto per la gestione assicurativa di specifici appalti relativamente alle polizze CAR, Fidejussioni, EAR e Decennale Postuma.

Condizioni:

- Importo minimo del valore dell'appalto/contratto pari ad €1.000.000;
- Mandato **esclusivo** ad Howden per la gestione assicurativa dell'appalto e libero da vincoli con altri intermediari;
- Invio bilancio depositato anno precedente (es: 2024);
- Previsionale anno in corso (es: al 31.12.2025);
- In caso di bilanci non soddisfacenti documentazione relativa ad ipotetici coobbligati;
- Documentazione completa di gara;
- Bando e Disciplinare (se presente);
- CSA (capitolato speciale di appalto);
- Schema di contratto;
- Cronoprogramma.



Claims Advisory perizie di parte

I nostri periti specializzati offrono una consulenza dedicata e specialistica per la risoluzione delle controversie sui sinistri occorsi alla proprietà con impatto sul business, con l'obiettivo di risolvere le controversie di carattere economico/contrattuale.

Tramite tale servizio forniamo perizie contrattuali di parte per tutte le tipologie di sinistri, svolte da professionisti interni, per aiutare il Cliente a gestire al meglio le emergenze.

Grazie ad una visione integrata, possiamo gestire gli interventi di emergenza e affiancare il Cliente nella fase di ricostruzione, fino alla negoziazione del miglior indennizzo.

Importanza della perizia di parte e vantaggi cliente

- Intervento tempestivo che consenta un supporto immediato al cliente che ha subito un sinistro rilevante.
- Aiutare il cliente per i primi interventi di salvataggio e bonifica in modo da consentire la ripartenza dell’attività nel più breve tempo possibile.
- Impostazione della pratica liquidativa analizzando tutta la documentazione di preesistenza e danno prima della consegna al perito della compagnia per evitare le problematiche con il perito della compagnia (es. Preesistenza su base cespiti spesso non corretta, descrizioni in fatture fuorvianti).
- Fidelizzazione del cliente.
- Il costo della perizia è molto spesso coperto dalla polizza con aggravi di costo nulli o minimi rispetto ai vantaggi.
- I fornitori che aderiranno alla convenzione potranno beneficiare di tariffe agevolate.

GRUPPO HERA

Hera_Pro EMPOWER

Insieme, per la crescita dei fornitori

CONTATTI

E-mail: fornitorihera@howdengroup.com
Telefono: +39 345 1468563

HOWDEN