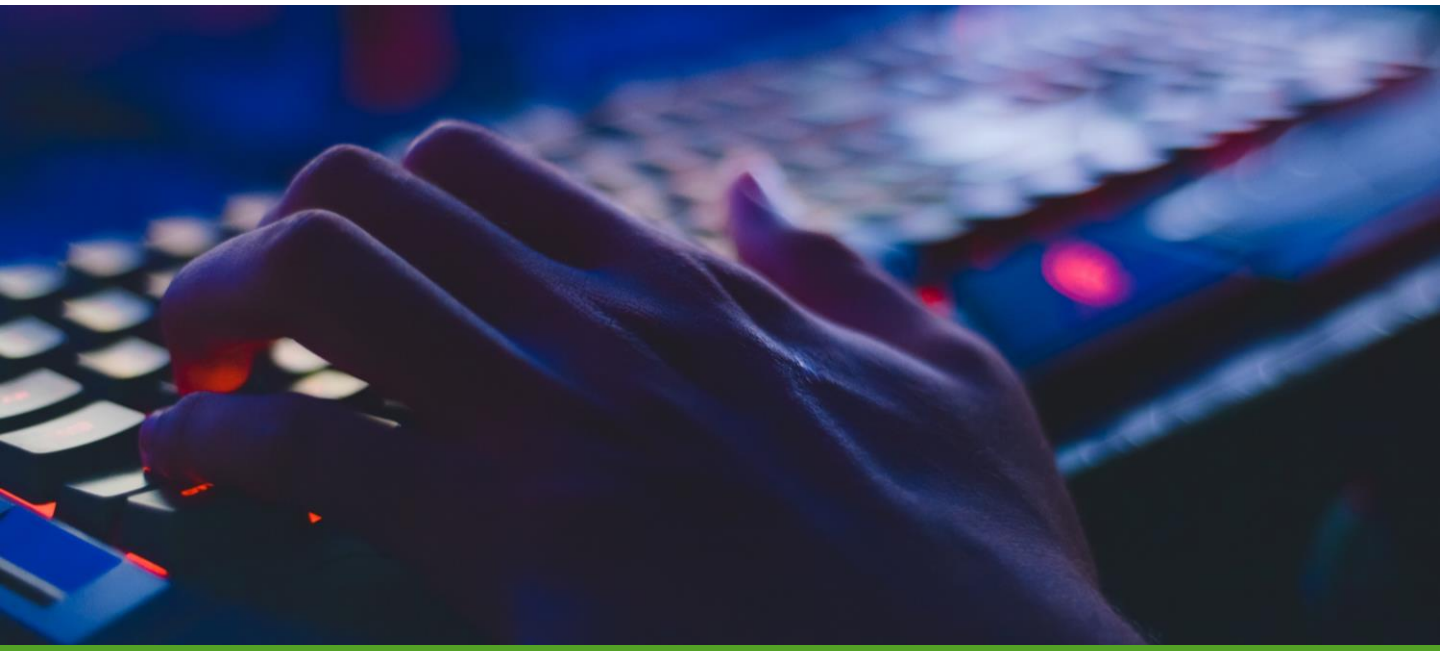
SECURITY 360

PROTECT YOUR BUSINESS

CATALOGO SERVIZI SECURITY 360

Soluzioni efficaci per la protezione della tua azienda



PROTEGGI IL TUO BUSINESS **CON I NOSTRI SERVIZI**

SECURITY 360

CHE COS'È LA CYBER SECURITY?

Facciamo un passo indietro e cerchiamo di capire che cos'è la Cyber Security.

Quando parliamo di sicurezza informatica facciamo riferimento a tutte quelle tecnologie utili a proteggere un sistema informatico, che sia un sistema di computer o un unico dispositivo, da tutti quegli attacchi che possono portare alla perdita o alla compromissione di informazioni e dati.

L'obiettivo quindi è molto semplice: **proteggere il cyberspazio dalle minacce.**

Queste minacce possono essere di tre diverse tipologie:

- **Cybercrimine:** avviene quando singoli attori o gruppi attaccano i sistemi per provocare interruzioni nelle attività aziendali o ottenere un ritorno economico
- **Cyberattacchi:** generalmente hanno lo scopo di raccogliere informazioni per finalità politiche
- **Cyberterrorismo:** mira a minare la sicurezza dei sistemi elettronici per suscitare panico

COME TI DIFENDIAMO DALLE MINACCE VIRTUALI E NON?

Ideiamo e implementiamo il miglior piano di sicurezza informatica per **proteggere il tuo business e la tua azienda** grazie alla partnership con figure esperte del settore.

Il percorso di **consulenza** prevede:

- Sicurezza fisica di controllo accessi
- Compliance procedure con consulenza e audit
- Formazione dei collaboratori
- Aspetto assicurativo per coperture danni
- Asset Vulnerabilities

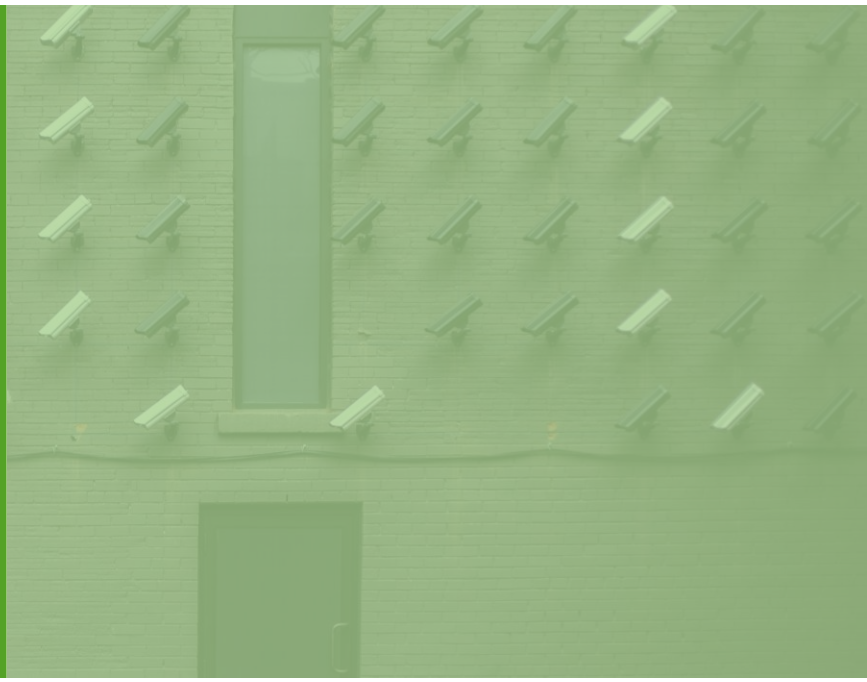
I servizi e le soluzioni **HRZ e Sigemi** per la sicurezza **garantiscono da oltre 10 anni la protezione a 360 gradi dei dati** delle aziende. Il nostro team testa l'infrastruttura del cliente e lo segue in tutto il percorso di crescita ed adeguamento strutturale.

Aiutiamo ad adottare **buone abitudini per proteggere al meglio l'azienda** con percorsi di formazione mirati rivolti alle risorse umane.

Security 360 infatti mette a disposizione un percorso utile a migliorare il livello di consapevolezza e di difesa dei dipendenti, nell'utilizzo quotidiano degli strumenti informatici.

#Security360 #WeareHRZ #Sigemi

I QUATTRO LIVELLI DI SERVIZO



GESTIONE DEGLI ACCESSI E VIDEO SORVEGLIANZA

Gestione della sicurezza delle persone e dei luoghi aziendali attraverso servizi hardware e software personalizzabili per ogni contesto.

GDPR COMPLIANCE MANAGEMENT

Servizi di tutela della violazione di leggi e regolamenti (nazionali e internazionali), norme aziendali e norme sociali.

SICUREZZA INFORMATICA A 360°

Procedure di cyber security e formazione ai collaboratori aziendali per prevenire e gestire possibili attacchi informatici.

SOFTWARE SAFETY & SECURITY

Sistema perfettamente integrato di soluzioni software per tutti gli aspetti relativi alla salute e alla sicurezza sul lavoro.

#Security360 #WeareHRZ #Sigemi

GESTIONE DEGLI ACCESSI E VIDEO SORVEGLIANZA

Gestione della **sicurezza delle persone e dei luoghi aziendali** attraverso servizi hardware e software personalizzabili per ogni contesto.

SOLUZIONI HARDWARE E SISTEMI INTEGRATI

Offriamo una vasta gamma di terminali per il controllo accessi, la video sorveglianza e per la sicurezza dei beni e del personale aziendale.

VULNERABILITY ASSESSMENT

Test utile per mettere alla prova la sicurezza dell'infrastruttura IT aziendale e di tutti i sistemi informatici, hardware e software.

#SECURITY360

SOLUZIONI HARDWARE

Incrementa il livello di sicurezza all'interno della tua azienda, **proteggi i tuoi beni con le nostre soluzioni hardware**. Disponiamo di una gamma completa di terminali, controller, lettori e accessori per il controllo accessi.

Facili da installare, immediati nell'utilizzo e dal design compatto ed elegante, i terminali Zucchetti, integrati al software di gestione accessi, garantiscono **un perfetto equilibrio operativo tra sicurezza, comfort e libertà di movimento.** La loro struttura compatta e robusta permette l'installazione dei dispositivi anche all'esterno.

SISTEMI INTEGRATI | per aumentare la sicurezza fisica

ANTIINTRUSIONE
Garantisce la sicurezza sia di ambienti piccoli che di grandi impianti industriali tramite notifiche di allarme immediate che permettono di intervenire tempestivamente in caso di pericolo.

ANTINCENDIO
Il sistema è in grado di allertare il personale di sicurezza consentendo altresì di indicare le vie di fuga e di raccogliere l'elenco dei presenti nei punti di raccolta in caso di evacuazione.

VIDEOSORVEGLIANZA
Piattaforma integrata per la gestione completa della videosorveglianza che permette la visualizzazione live dei siti controllati e l'analisi video comportamentale. È possibile anche autorizzare o negare gli accessi da remoto mediante funzionalità semi automatiche.

LETTURA TARGHE
Sistema basato su una telecamera per il riconoscimento di lettura delle targhe di auto, moto e veicoli in genere. La soluzione è in grado di gestire e archiviare le informazioni registrate da ogni telecamera e di consentire o meno l'ingresso nelle aree di transito e sosta.

GESTIONE PUNTI DI RACCOLTA
Soluzione che attraverso l'utilizzo di badge e terminali consente di accertarsi che in caso di emergenza tutti i lavoratori abbiano lasciato la struttura e raggiunto i punti di raccolta.

GESTIONE VISITATORI
Gestione sicura ed efficace dei flussi di accesso dei visitatori grazie alla modalità automatica di self check-in.

#SECURITY360

VULNERABILITY ASSESSMENT

Il vulnerability assessment è il pilastro centrale per qualsiasi strategia di sicurezza proattiva!

Si tratta di un test utile per **mettere alla prova la sicurezza** dell'infrastruttura IT aziendale e di tutti i sistemi informatici, hardware e software.

Questo servizio non è un semplice test, quanto più **insieme di attività di scansione della rete** che permette di individuare e classificarne le vulnerabilità che potrebbero essere il potenziale punto d'accesso per degli attacchi informatici.

Le moderne valutazioni delle vulnerabilità si basano su strumenti di scansione automatizzati. Qui sotto l'elenco delle principali categorie di strumenti utilizzati per scansionare un ambiente alla ricerca di vulnerabilità:

Scansione basata sulla rete e sulla rete Wi-Fi: utilizzata per identificare potenziali attacchi alla sicurezza della rete.

Scansione basata su host: utilizzata per identificare le vulnerabilità su server, workstation o altri host di rete.

Scansioni delle applicazioni: utilizzate per testare siti Web e applicazioni mobili per vulnerabilità software note e configurazioni errate.

Scansioni del database: utilizzate per identificare le vulnerabilità che potrebbero consentire attacchi specifici del database.

Completata la scansione cosa succede?

Viene generato un report che, oltre a elencare le vulnerabilità identificate e la loro potenziale gravità d'impatto, fornisce le raccomandazioni per mitigare o porre rimedio a ciascuna di esse, **al fine di quantificare e prioritizzare le misure da adottare.** Parte della consulenza è il supporto alla redazione di un piano di correzione, che affronterà le vulnerabilità nell'ordine corretto, in funzione di gravità, probabilità di sfruttamento, potenziale impatto aziendale e difficoltà di bonifica.

GDPR COMPLIANCE MANAGEMENT

Servizi di tutela della **violazione di leggi e regolamenti** (nazionali e internazionali), norme aziendali e norme sociali.

GESTIONE PRIVACY GDPR

Questo servizio tratta la tutela dei dati personali e sensibili in linea con le ultime normative europee.

#SECURITY360

GESTIONE PRIVACY GDPR

SEI TU A SCEGLIERE
IL TUO SUPPORTO
IDEALE

Questo servizio tratta la tutela dei dati personali e sensibili in linea con le ultime normative europee. Lo scenario legislativo italiano prevede **obblighi stringenti** relativamente alla **tutela della privacy.**

Grazie a collaborazioni consolidate con consulenti e legali specializzati in materia di privacy, **ti offriamo consulenze complete per l'adeguamento dei processi aziendali** alle direttive imposte dal General Data Protection Regulation (GDPR).

Qual è il valore aggiunto del nostro servizio?

Lo costruiamo insieme a te, modellandolo sulle peculiarità del modello di business e di organizzazione della tua azienda.

L'adeguamento al GDPR ha differenti finalità e vantaggi

- **Adempiere ad un Regolamento europeo**, obbligatorio verso tutti coloro che acquisiscono e conservano dati personali per fini di carattere professionale, quindi sia di clienti che di dipendenti;
- **Tutelarsi dagli effetti dannosi** che comporterebbe la perdita dei dati personali sia sotto il profilo dell'immagine aziendale, sia sotto l'aspetto delle domande risarcitorie che i titolari dei dati hanno diritto di richiedere;
- **Evitare le ingenti sanzioni** che il legislatore UE ha previsto in caso di violazioni del GDPR, fino al 4% del fatturato del professionista.

#Security360 #WeareHRZ #Sigemi

SICUREZZA INFORMATICA A 360°

Procedure di **cyber security** e formazione ai collaboratori aziendali per prevenire e gestire possibili attacchi informatici.

RISK ASSESSMENT PER LA VALUTAZIONE DEL RISCHIO

Servizio di check-up che rileva ogni possibile rischio o minaccia a cui è sottoposta la tua azienda.

SIMULAZIONE DEI PHISHING

L'attacco phishing viene fatto online tramite messaggi ingannevoli per portare le vittime a condividere dati sensibili.

PENETRATION TEST

Si tratta di un test della sicurezza dell'infrastruttura IT.

CONSULENZA CYBER SECURITY

Consulenza specializzata in un percorso di formazione finalizzato all'ottimizzazione della tua infrastruttura IT.

FORMAZIONE CYBER SECURITY

La formazione del personale su come identificare e prevenire le minacce è fondamentale per la sicurezza dell'azienda.

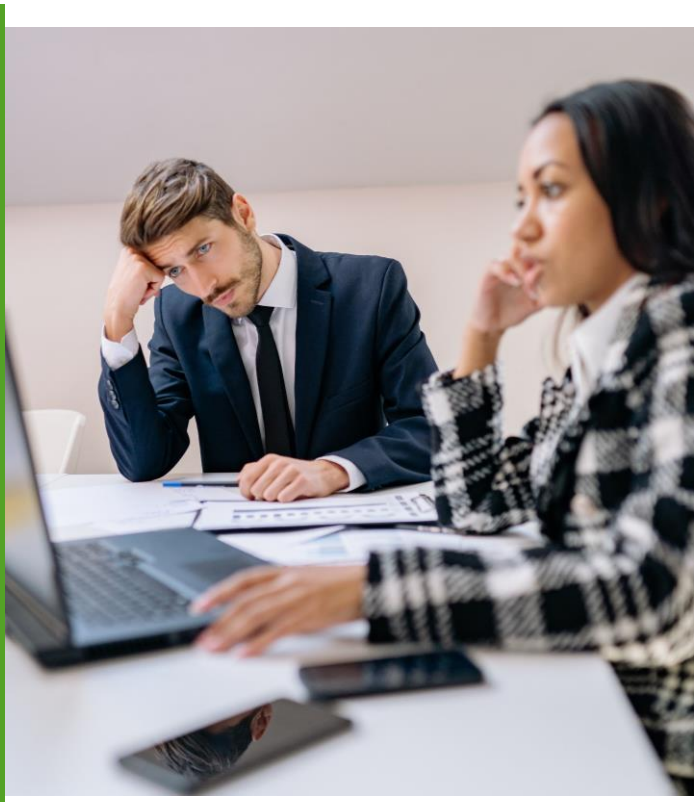
#Security360 #WeareHRZ #Sigemi

#SECURITY360

RISK ASSESSMENT PER LA VALUTAZIONE DEL RISCHIO

Avere una visione chiara delle minacce che possono intaccare l'integrità del sistema informativo aziendale è fondamentale per poterle bloccare.

La si può ottenere con il servizio di Check-up che rileva ogni possibile rischio o minaccia a cui è sottoposta la tua azienda. **Il passo successivo è quello di studiare un piano di azione per fronteggiare i possibili attacchi.**



La procedura si divide in **tre fasi principali**: individuazione e **analisi** del contesto e dei processi aziendali, **individuazione** dei possibili rischi a cui un'azienda è esposta e infine la **valutazione** dei rischi individuati da un punto di vista sia qualitativo che quantitativo.

Individuare e valutare correttamente i rischi a cui un'azienda è esposta **non solo aiuta a evitare inconvenienti, ma permette anche di gestire in modo migliore e più consapevole le proprie risorse.**

TIP | alcuni consigli per proteggersi dagli attacchi

Per salvaguardarsi dagli attacchi informatici le imprese o i singoli utenti possono ricorrere ad alcune semplici strategie e strumenti:

1 - Eseguire periodicamente un backup di tutti i dati aziendali

#SECURITY360

SIMULAZIONE DEI PHISHING

Il phishing simulation è una simulazione che **riproduce un attacco di Phishing all'interno della rete aziendale,** al fine di verificare il grado di preparazione e consapevolezza dei collaboratori.

Al termine dell'operazione di simulazioni si potrà capire **quel è il livello medio di resistenza** agli attacchi phishing di tutta l'organizzazione.

TIP | alcuni consigli per proteggersi dagli attacchi

Per salvaguardarsi dagli attacchi informatici le imprese o i singoli utenti possono ricorrere ad alcune semplici strategie e strumenti:

2 - Tenere aggiornati il software e il sistema operativo per sfruttare le patch di sicurezza più recenti

Il phishing funziona perché inganna le persone a fare cose che vanno a vantaggio del criminale informatico che ha inviato l'e-mail dannosa. Per esempio, l'email phishing tipicamente **usa stratagemmi come far sentire il destinatario preoccupato che se non clicca su un link potrebbe finire nei guai al lavoro.**

Le condizioni che suscitano paura, incertezza e dubbio, insieme all'urgenza, e altri trucchi psicologici fanno del phishing il metodo numero uno per iniziare un attacco informatico. I dipendenti devono capire questi astuti trucchi di phishing per avere la possibilità di resistere all'impulso **di cliccare su un link dannoso o scaricare un allegato infetto.**

#Security360 #WeareHRZ #Sigemi

#SECURITY360

PENETRATION TEST

Si tratta di un test della sicurezza dell'infrastruttura IT. Attività condotta da una squadra di specialisti, che evidenzia le criticità del sistema e **verifica l'entità dell'impatto di un attacco reale.**

Attraverso questo servizio **si riescono ad identificare e classificare le vulnerabilità dell'infrastruttura IT** aziendale, l'adeguatezza delle policies di sicurezza e il loro effettivo rispetto.

Il vantaggio principale dell'eseguire un Penetration Test è sicuramente **la possibilità di verificare in tempo reale la validità dei sistemi di difesa e correre così ai ripari per sanare ogni falla**. I benefici però sono tanti e una corretta attività di testing, se eseguita correttamente, può davvero aiutare un'azienda a capire che direzione prendere per lavorare sicuri a 360 gradi.

Innanzitutto **compiere un'analisi** è utile per valutare se le politiche di sicurezza aziendali sono comprese e rispettate da tutti i dipendenti: **gli attacchi esterni sono sempre dietro l'angolo**, ma spesso i malfunzionamenti partono proprio dall'interno ed è bene educare il personale perché adotti un comportamento adeguato e rispettoso delle norme di sicurezza.

Un altro vantaggio dell'esame **è la capacità di individuare le irregolarità** che potrebbero causare interruzioni di servizio, paralizzando l'attività e causando grosse perdite economiche.

TIP | alcuni consigli per proteggersi dagli attacchi

Per salvaguardarsi dagli attacchi informatici le imprese o i singoli utenti possono ricorrere ad alcune semplici strategie e strumenti:

3 - Installare un valido antivirus in grado di eliminare e rimuovere le minacce

#SECURITY360

CONSULENZA CYBER SECURITY

La **digital transformation** impone alle aziende di ricorrere sempre più alla digitalizzazione per potersi relazionare con clienti, fornitori e partner.

Per questo motivo **il livello di attenzione alla sicurezza Informatica si è evoluto**, soprattutto dopo l'entrata in vigore di determinate normative Europee (GDPR), che richiedono alle aziende ulteriori verifiche sulla sicurezza della loro infrastruttura.

Il servizio offerto consiste in una consulenza specializzata e in un **percorso di formazione finalizzato all'ottimizzazione della tua infrastruttura IT.**

Con questo servizio **forniamo una panoramica globale** dell'evoluzione degli scenari che coinvolgono il mondo digitale, le nuove minacce e il modo in cui difendersi.

TIP | alcuni consigli per proteggersi dagli attacchi

Per salvaguardarsi dagli attacchi informatici le imprese o i singoli utenti possono ricorrere ad alcune semplici strategie e strumenti:

4 - Utilizzare password complesse e reti Wi-Fi protette

#Security360 #WeareHRZ #Sigemi

RENDI SICURA LA
TUA AZIENDA
INVESTI NELLA
FORMAZIONE

FORMAZIONE CYBER SECURITY

La formazione del personale su come identificare e prevenire le minacce è fondamentale per la sicurezza dell'azienda. Proprio per questo **è opportuno formare il personale a tutti i livelli** in modo da abbassare il rischio di attacco e compromissione. Proponiamo diversi corsi di cyber security erogabili in presenza oppure attraverso webinar online.

La didattica dei corsi è studita per **spiegare in modalità molto semplici (non tecniche)** tutte quelle tipologie di attacco che sfruttano l'anello debole della catena, ovvero il fattore umano.

3 ASPETTI PER UNA CORRETTA FORMAZIONE

AWARENESS | Conoscenza è consapevolezza. Questo elemento va ricercato all'interno di qualsiasi corso sulla sicurezza informatica.

TRAINING | La formazione di sicurezza informatica deve fortemente tenere conto dell'aspetto pratico.

PROCESSI DI LEARNING | Fornire gli strumenti per costruirsi seppur parzialmente le competenze per rispondere agli eventi inattesi che nella cybersecurity sono all'ordine del giorno.

TIP | alcuni consigli per proteggersi dagli attacchi

Per salvaguardarsi dagli attacchi informatici le imprese o i singoli utenti possono ricorrere ad alcune semplici strategie e strumenti:

5 - Non fare clic su allegati email di mittenti sconosciuti

#Security360 #WeareHRZ #Sigemi

SOFTWARE SAFETY & SECURITY

Sistema perfettamente integrato di soluzioni software **per tutti gli aspetti relativi alla salute e alla sicurezza sul lavoro**.

Valutazione dei rischi e DVR

Il software che ti permette di redigere il DVR, pianificare tutte le misure preventive e protettive, verificarne l'attuazione e gestirle nel tempo, grazie all'applicazione di un vero e proprio sistema di audit interno.

Sorveglianza sanitaria

Il software che risponde alle disposizione dell'art. 41 del D. lgs. 81/08 in materia di medicina del lavoro e che semplifica l'attività dell'azienda e del Medico Competente.
Grazie al sistema di alert automatici garantisce inoltre il pieno controllo e il rispetto delle scadenze: idoneità del lavoratore, nomine del Medico Competente, vaccinazioni a cui il lavoratore deve essere sottoposto, ecc.

Adempimenti formativi

Il software per gestire al meglio la formazione dei collaboratori in materia di salute e sicurezza sul lavoro, sia che si tratti di incontri in aula, di distribuzione di materiale informativo o di addestramento sul campo.

Gestione appalti e qualifica fornitori

La sicurezza sul lavoro non deve essere gestita solo in merito ai collaboratori e ai processi aziendali, ma anche alle interferenze che nascono quando in azienda accedono aziende terze o lavoratori autonomi, per i quali il datore di lavoro diventa responsabile. Il software consente di gestire in modo estremamente semplice l'iter di qualifica dei fornitori e la relativa valutazione, definire quali documenti e certificazioni il fornitore deve esibire e gestire le scadenze.

Perché scegliere I NOSTRI SERVIZI

HRZ & SIGEMI

Il team HRZ si compone di consulenti altamente specializzati e preparati, che hanno affiancato oltre 1.000 realtà nel **raggiungimento degli obiettivi strategici ed operativi** dell'organizzazione aziendale.

Favoriamo così la **valorizzazione del capitale umano**, migliorando la produttività di tutti i collaboratori nonché la pianificazione, gestione e monitoraggio delle attività del personale aziendale e l'ottimizzazione delle risorse sia umane che economiche e finanziarie investite nei processi di produzione, ricerca e sviluppo, vendita, marketing e contabili.

A queste competenze in ambito HR **abbiamo voluto affiancare l'expertise di Sigemi**, nostro partner tecnologico in grado di supportare le aziende per il raggiungimento degli obiettivi di efficienza aziendale.

Sigemi offre consulenza informatica, servizi per l'ottimizzazione delle performance degli applicativi Zucchetti, soluzioni in cloud e assistenza sistemistica.

Grazie al suo **team di professionisti, con pluriennale esperienza nel settore della consulenza informatica** e assistenza sistemistica, Sigemi **si prende cura dell'infrastruttura IT delle aziende**, mettendo a disposizione strumenti efficienti per aumenta la produttività e facilitare il raggiungimento degli obiettivi aziendali.

Specializzata nel disegno e nell'implementazione di servizi Cloud, Sigemi è in grado di consigliare la **migliore soluzione**.

Il ventaglio di servizi offerti è ampio e variegato e caratterizzato da un alto grado di flessibilità e da un approccio personalizzato, accompagnando l'azienda nel passaggio tecnologico.

Grazie se ci vorrai rendere il tuo PARTNER tecnologico di riferimento.

#Security360 #WeareHRZ #Sigemi

SECURITY 360
PROTECT YOUR BUSINESS

I NOSTRI CONTATTI

Contattaci per avere maggiori informazioni e per progettare insieme il tuo livello di servizio ottimale.

HRZ Milano
HR Top Partner Zucchetti
E-mail: commerciale@hrz.it
Telefono: 02.45.48.08.81
www.hrz.it

Follow us
LinkedIn | Facebook | Instagram | YouTube

Sede di Milano
Via Brembo, 23
20139 - Milano (MI)

Sede di Torino
Corso Unione Sovietica, 612/21
10035 - Torino (TO)

Sede di Brescia
Via Creta, 31
25124 - Brescia (BS)

> Visita il sito **Sigemi**
> **www.sigemi.it**