David Scaffaro
STUDIO DI CONSULENZA
Consulenza normativa, legislativa e di Direzione

Cyber Security

Legislazione, normativa e standard internazionali

WHITE PAPER

APR 2023

David Scaffaro - Studio di consulenza normativa, legislativa e di Direzione
P. IVA: 06560021005 - Via S. Quasimodo,30 00144 Roma - Tel. 334/9251259 - www.stdsconsult.com - email: davidscaffaro@yahoo.it

2

Cyber security

Introduzione.

Con l'avanzamento della tecnologia, la cyber security è diventata una preoccupazione crescente per le persone, le aziende e le organizzazioni di tutto il mondo. La protezione dei dati sensibili, e la sicurezza nell'accesso ai sistemi informatici, sono ora più importanti che mai, poiché le minacce informatiche diventano sempre più sofisticate. La cyber security è la pratica di proteggere i sistemi informatici, i dati e le reti da attacchi informatici, dalla violazione della privacy e da altre minacce informatiche.

Strategia per la sicurezza

Una delle componenti più importanti della cyber security è la strategia per la sicurezza. Questo tipo di strategia comprende l'analisi dei rischi, la definizione di obiettivi di sicurezza, la selezione di controlli appropriati, la pianificazione delle attività e la valutazione delle prestazioni e dei feedback. Si tratta di un processo che deve essere continuamente aggiornato, per tenere il passo con le minacce informatiche le quali sono sempre in rapida evoluzione. La strategia deve essere definita a livello aziendale e applicata a tutti i livelli.

Protezione dei dati sensibili

Un aspetto importante della cyber security è quello di proteggere i dati sensibili. I dati sensibili sono informazioni riservate, e comunque regolati secondo la pertinente definizione richiamata nel GDPR. I dati sensibili possono includere l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, informazioni relative alla salute o alla vita sessuale. Per proteggere questi dati, è necessario implementare solide misure di sicurezza, come l'autenticazione a più fattori, la crittografia dei dati e l'isolamento dei dati sensibili.

3

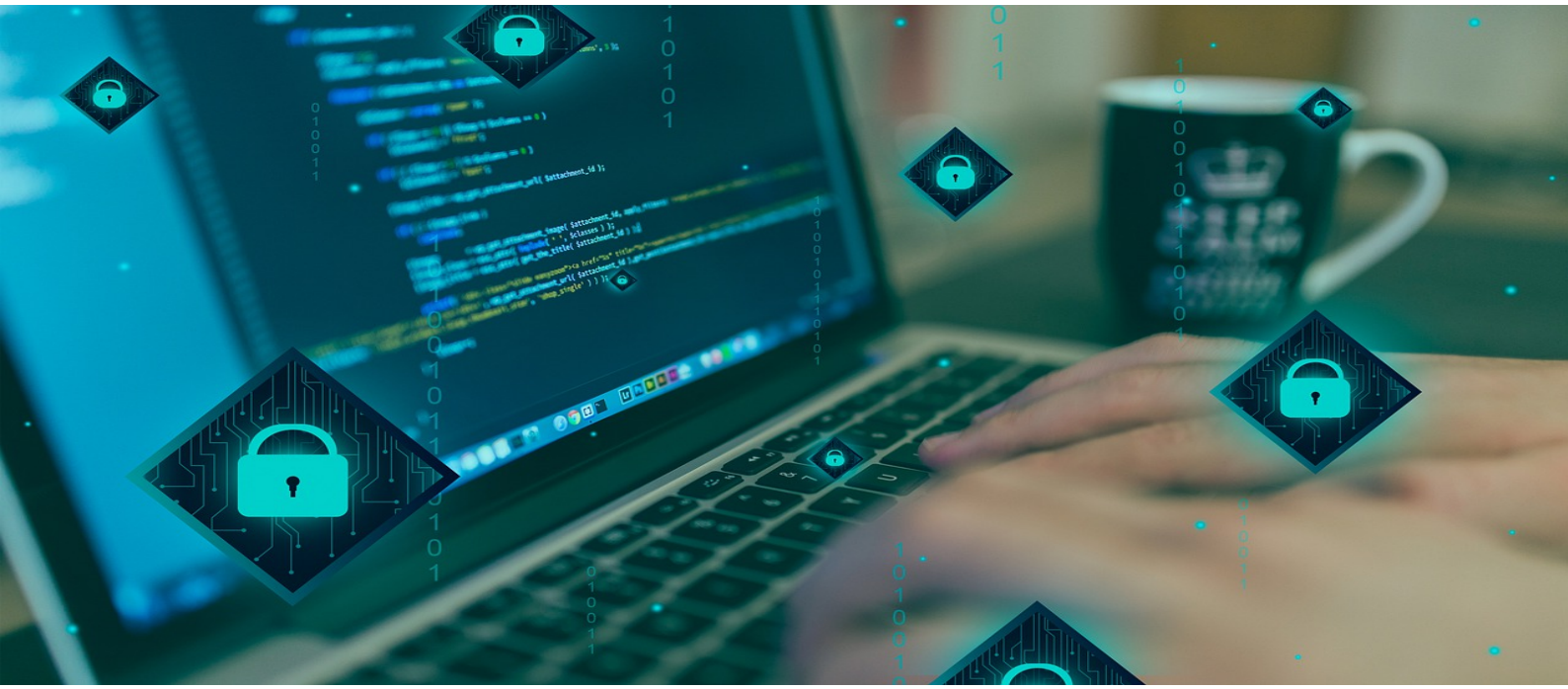
Cyber security

Conoscere le principali minacce informatiche

Un'altra parte fondamentale della cyber security è conoscere le principali minacce informatiche. Le minacce informatiche sono una delle più grandi sfide che i sistemi informatici devono affrontare oggi. Queste minacce sono reali e crescenti in termini di complessità e portata. Tra queste possiamo citare, ad esempio, il malware, le tecniche di phishing o di hacking e il social engineering.

Conclusione

La cyber security è una pratica importante e in continua evoluzione. La creazione di una strategia di sicurezza, la protezione dei dati sensibili e la conoscenza delle principali minacce informatiche sono tutti aspetti importanti della cyber security. La comprensione di questi principi fondamentali può aiutare le persone e le Organizzazioni a proteggere i propri sistemi informatici, i dati e le reti da attacchi informatici, violazioni della privacy e altre minacce informatiche.



4

Cyber security

Aspetti legislativi.

I due adempimenti principali in tema di cyber security, a cui le Organizzazioni sono soggette, sono riscontrabili nel GDPR (Regolamento UE 679/16) e nel D.Lgs. 231/01, negli articoli di pertinenza che descrivono i reati informatici (art. 24 e 24-bis).

Si tratta di legislazioni severe, le quali presentano un articolato e incisivo impianto sanzionatorio (vedere pagina 12).

Ulteriori legislazioni di interesse sono la Legge n. 48/2008 (ratifica della Convenzione Budapest del 23/11/2001, del Consiglio d'Europa sulla criminalità' informatica) e il codice dei consumatori (con le modifiche apportate dal D.L. 14 gennaio 2023, n. 5, convertito, con modificazioni, dalla L. 23/2023, dal D.Lgs. 26/2023 e dal D.Lgs. 28/2023.

5

Cyber security – GDPR

Focus su temi relazionati alla cyber security.

L'articolo 32 del Regolamento Generale sulla Protezione dei Dati (GDPR) riguarda la sicurezza dei dati. Prevede che le Organizzazioni che trattano i dati personali, prendano misure appropriate per garantire la sicurezza dei dati stessi, con una serie di misure tecniche e organizzative. Tali misure devono essere adeguate al rischio, tenendo conto dello stato della tecnologia,dei costi di attuazione della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché dei rischi diversi per i diritti e le libertà delle persone fisiche.

Le misure devono comprendere, in particolare, la protezione contro l'elaborazione non autorizzata o illecita, la perdita dei dati, la distruzione o l'alterazione accidentale. Inoltre, le Organizzazioni che trattano i dati devono documentare le misure adottate in modo da dimostrare l'osservanza del GDPR.

Tali misure devono essere soggette a una valutazione periodica, al fine di verificare la loro efficacia. Infine, le Organizzazioni devono adottare misure adeguate per garantire che solo le persone autorizzate possano accedere ai dati personali.

6

Cyber security – D.Lgs. 231/01

Focus su temi relazionati alla cyber security.

Il Decreto Legislativo 231/01 disciplina la responsabilità amministrativa delle persone giuridiche in caso di reati. Nello specifico, il Decreto contiene disposizioni relative anche ai reati informatici, che sono stati introdotti all'interno della disposizione e richiamati negli art. 24 e 24-bis.
I reati informatici disciplinati dal Decreto 231/01 riguardano principalmente le violazioni della sicurezza informatica e le frodi informatiche a danno dello Stato. Inoltre, sono previsti reati relativi alla produzione e al commercio di software pirata, all'utilizzo improprio delle reti, all'interruzione o alla manipolazione dei servizi di comunicazione elettronica, nonché alla diffusione di informazioni false o ingannevoli.

Nel D.Lgs. 231/2001 vengono anche affrontati reati relazionabili alla violazione della privacy, seppur in modo indiretto, in particolare con riferimento all'utilizzo improprio dei dati personali.

In conclusione, il Decreto Legislativo 231/2001 contiene disposizioni a tutela della sicurezza informatica, nonché misure volte a prevenire e punire i reati informatici. Il compimento di tali disposizioni rappresenta un importante strumento nelle mani delle Organizzazioni, atto a prevenire e contrastare i suddetti reati.

7

Cyber security

Aspetti sugli standard volontari.

Oltre alle disposizioni di legge vigenti, esistono diversi standard internazionali, di tipo volontario, che trattano temi relativi alla cyber security, sotto diverse sfumature ed ambiti.

Questi rappresentano eccellenti strumenti, atti a gestire i rischi derivanti dai pericoli in ambito di cyber security, contribuendo a minimizzare danni, perdite, risarcimenti, fermo delle attività od altri eventi negativi.

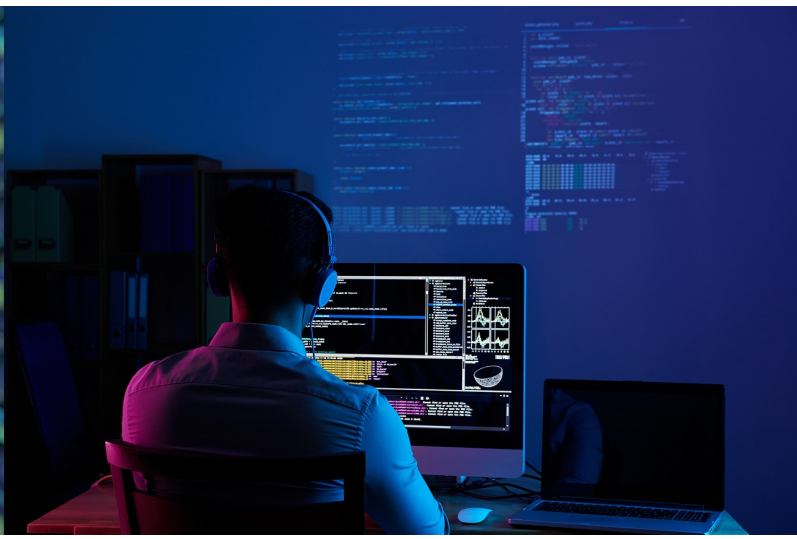
Di seguito alcuni tra i maggiori standard:

- **ISO 27001** “Information security management systems”

- **ISO 22301** "Societal security - Business continuity management systems — Requirements"

- **ISO 21434** “Road vehicles — Cybersecurity engineering”

- **ISO 27032** “Information technology — Security techniques — Guidelines for cybersecurity”



8

Cyber security – ISO 27001

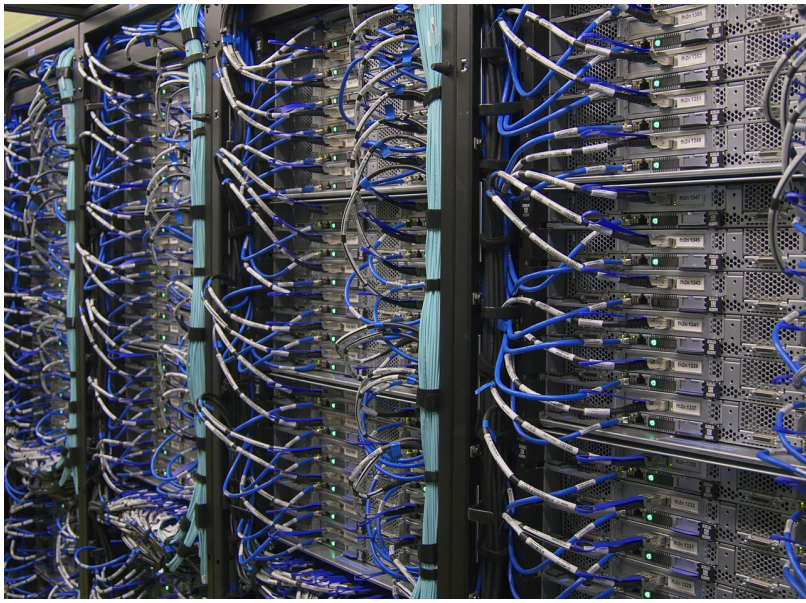
ISO 27001 “Information technology - Security techniques - Guidelines for cybersecurity”

La norma ISO 27001 è uno standard globale, riconosciuto a livello internazionale, che definisce le metodologie migliori per gestire la sicurezza delle informazioni. È uno standard fondamentale per le organizzazioni che desiderano preservare la riservatezza, l'integrità e la disponibilità dei dati. La norma ISO 27001 definisce un quadro dettagliato per la gestione della sicurezza delle informazioni, offrendo soluzioni pratiche per la protezione dei dati sensibili all'interno di un'organizzazione. La norma fornisce una guida specifica per l'implementazione delle misure di sicurezza informatica, fornendo una base affidabile su cui le organizzazioni possono contare per la protezione dei dati.

9

Cyber security – ISO 22301

ISO 22301 "Societal security - Business continuity management systems - Requirements"



La norma ISO 22301 fornisce le linee guida per la gestione della continuità aziendale. È uno standard internazionale per la preparazione, la pianificazione, l'implementazione, la verifica e il miglioramento della continuità aziendale. La norma fornisce un sistema di gestione della sicurezza che aiuta le organizzazioni a identificare e mitigare i rischi che potrebbero interrompere le loro operazioni ed attività. La norma può aiutare le organizzazioni a gestire le minacce alla continuità aziendale, ad adottare un approccio proattivo alla gestione dei rischi e a garantire che le loro attività siano svolte in modo efficiente.

I vantaggi dell'implementazione della norma ISO 22301 includono una maggiore sicurezza dei dati, una migliore resilienza alle minacce alla continuità del business e una maggiore competitività.

10

Cyber security – ISO 21434

ISO 21434 "Road vehicles - Cybersecurity engineering"

La norma ISO 21434 è uno standard internazionale che delinea le linee guida per la sicurezza delle infrastrutture di trasporto connesso. Si tratta di una guida fondamentale per i produttori, i fornitori di servizi e i proprietari di veicoli connessi che desiderano garantire la sicurezza dei propri sistemi. La norma definisce i requisiti di sicurezza per la progettazione, la costruzione, l'installazione, l'utilizzo, la manutenzione e l'esercizio dei veicoli connessi. Include anche le regole e le procedure per la gestione della sicurezza per tutti gli aspetti dell'infrastruttura di trasporto connessa. La norma è uno strumento essenziale per aiutare le aziende produttrici a promuovere la sicurezza dei veicoli connessi.

11

Cyber security – ISO 27032

ISO 27032 "Information technology - Security techniques - Guidelines for cybersecurity"

La norma ISO 27032 è uno standard internazionale che definisce le linee guida per la gestione della sicurezza delle informazioni e della cybersecurity. La norma fornisce una visione completa delle soluzioni di sicurezza da implementare al fine di tutelare la sicurezza delle informazioni e raggiungere un livello di sicurezza accettabile nell'organizzazione. La norma offre una guida per la gestione del rischio informatico, la gestione della sicurezza dei dati, la gestione della cybersecurity, la gestione della privacy, la gestione dell'accesso e la gestione della sicurezza delle reti. La ISO 27032 offre importanti suggerimenti e linee guida su come gestire la sicurezza informatica in un modo professionale e sicuro.

Cyber security - sanzioni

Sanzioni

Adempimento	**Amministrative**	**Penali**	**Interdittive**
D.Lgs. 231/01			
Art. 24	Da 51.600 a 929.400 euro	Si, pene variabili a seconda dei reati	Si (sospensione dell'attività, da 3 mesi a 2 anni, fino all'interdizione definitiva)
Art.24-bis	Da 25.800 a 774.500 euro	Si, pene variabili a seconda dei reati	Si (sospensione dell'attività, da 3 mesi a 2 anni, fino all'interdizione definitiva)
GDPR			
Art. 83	Da 10.000.000 a 20.000.000 euro *	Si, pene variabili a seconda dei reati **	Si (limitazione o divieto del trattamento dei dati)

* oppure dal 2% al 4% del fatturato mondiale nel caso sia superiore al valore di 10 M e 20 M di euro. Il GDPR non prevede un valore minimo per la sanzione, che pertanto dovrà essere commisurata dall'Autorità Garante sulla base dei criteri di effettività, proporzionalità e dissuasività.

** si faccia riferimento al D.Lgs. 101/18

David Scaffaro - Studio di consulenza normativa, legislativa e di Direzione
P. IVA: 06560021005 - Via S. Quasimodo,30 00144 Roma - Tel. 334/9251259 - www.stdsconsult.com - email: davidscaffaro@yahoo.it

Cyber security - Cosa possiamo fare

Abbattiamo i rischi sanzionatori e la gap compliance.

L'esperienza ultra ventennale sui temi legislativi d'impresa, ci consente di abbattere i rischi di sanzioni amministrative, penali e interdittive per le aziende italiane oppure estere che operino sul mercato italiano.

Valutiamo la gap compliance, verificando il grado di adempimento aziendale e confrontandolo con la situazione ottimale in cui dovrebbe trovarsi l'azienda per minimizzare i rischi.

Sulla base delle caratteristiche aziendali e in riferimento ai diversi ambiti legislativi su cui possiamo intervenire, prepariamo la documentazione richiesta dagli obblighi e procedurizziamo i processi a rischio, con estrema attenzione alle casistiche che possano portare al compimento di reati.

Visto il rapido e continuo mutare del quadro normativo e legislativo, forniamo alle aziende assistenza nel tempo, al fine di mantenere allineata la documentazione alle successive modifiche e integrazioni di legge, oppure a variazioni dei processi aziendali.

Vi seguiamo e supportiamo nell'iter certificativo.

L'esperienza accumulata negli anni, derivante dall'elaborazione di centinaia di sistemi di gestione, sia su standard ISO che extra ISO, ci consente di portarvi agevolmente all'ottenimento dei più importanti standard di settore.

Ci occupiamo di redarre la documentazione, di gestire i rapporti con l'Ente di Certificazione e di assistervi nella verifica, sia da remoto che in presenza.

Forniamo assistenza nel tempo, redigendo la documentazione richiesta nelle verifiche di sorveglianza.

Possiamo utilizzare le certificazioni per rafforzare, tramite adeguate procedure, la compliance legislativa di qualsiasi Organizzazione.

Lavoriamo esclusivamente con Enti di Certificazione accreditati Accredia e/o UKAS, per garantire al cliente la validità internazionale dei certificati emessi.

Ad oggi, i nostri sistemi documentali sono stati certificati dai maggiori Enti di Certificazione, sia nazionali che internazionali.

David Scaffaro - Studio di consulenza normativa, legislativa e di Direzione
P. IVA: 06560021005 - Via S. Quasimodo,30 00144 Roma - Tel. 334/9251259 - www.stdsconsult.com - email: davidscaffaro@yahoo.it

David Scaffaro
STUDIO DI CONSULENZA
Consulenza normativa, legislativa e di Direzione

P. IVA: 06560021005 - Via S. Quasimodo,30 00144 Roma - Tel. 334/9251259 - www.stdsconsult.com - email: davidscaffaro@yahoo.it

APR 2023