ISP N° 0443 E

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC

Signatory of EA, IAF and ILAC Mutual Recognition Agreements

GERICO SECURITY SRL

ORGANISMO DI ISPEZIONE

REGOLAMENTO PER LE ATTIVITÀ ISPETTIVE A NORMA ISO/IEC 17020

Documento preparato da:	Giustino Fumagalli
Documento verificato da:	CDA
Data:	04/07/2023
Versione:	3.0

Versione	Data	Note esplicative
1.0	01/02/2020	Prima emissione
1.1	13/03/2021	Aggiornamento a seguito dei rilievi di Accredia del 04/03/2021
1.2	01/08/2021	Aggiornamento a seguito DPCM 81 del 14/04/2021 pubblicato il 11/06/2021
1.3	29/12/2021	Revisione a conclusione visita Accredia e Accreditamento
1.4	29/10/2022	Revisione a seguito del 1* Audit Accredia
2.0	04/01/2023	Introduzione del Vulnerability Scan durante l'Ispezione
3.0	*04/07/2023*	*Introduzione del Executive Report*

Sommario

1 GENERALE

1.1 Premessa

Gerico Security Srl con sede legale in via Antonio Gambacorti Passerini, 2 Monza (MB), tramite la sua Direzione denominata "Organismo di Ispezione"[1], svolge ispezioni conformemente alla ISO/IEC17020, in merito alla sicurezza delle informazioni e cyber presso qualsiasi tipologia di organizzazione privata o pubblica.
Con Ispezione si intende "l'esame di un processo, di un servizio, o di una loro progettazione, e determinazione della sua conformità a requisiti specifici o, sulla base di un giudizio professionale, a requisiti generali"[2].

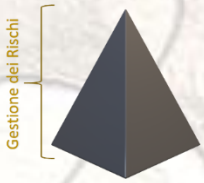
1.2 Scopo e Campo di applicazione

Scopo del presente regolamento è quello di disciplinare le condizioni e le modalità di esecuzione dei servizi ispettivi da parte dell'Organismo di Ispezione (OdI) di Gerico Security Srl, che riguardano nello specifico a:

Schema	Category	Field	Subfield	Range	Stage	Requirements
ISP	Processo/ Servizio	Information and Communications Technology	//	Ispezioni e verifiche sulla sicurezza delle informazioni e cybersecurity	• Prima dell'avvio del servizio • In servizio	Cyber Security Framework Nazionale – CSF 2.0 Febbraio 2019
ISP	Process/ Service	Information and Communications Technology	//	Inspection and verification on information security and cybersecurity	• Pre service • In service	Cyber Security Framework Nazionale – CSF 2.0 Febbraio 2019

Tutti i processi collegati alle ispezioni, ivi inclusi la gestione degli ispettori e il mantenimento di un Archivio di Ispezione sono da considerarsi all'interno del campo d'applicazione.

L'Organizzazione viene ispezionata al fine di fotografare la situazione in essere secondo quattro direttrici, tre direttrici alla base della Piramide della Cyber Security e una corrispondente all'altezza della Piramide come illustrato nelle figure sottostanti:



[1] Gerico Security Srl in riferimento alla ISO/IEC 17020:2012 svolge le ispezioni quale Organismo di Ispezione di Tipo C (Cfr.ISO/IEC17020 clausola 4.1.6 (c)) Accreditato da Accredia

[2] Contestualizzazione della definizione di Ispezione presente nella ISO 17000:2020 (6.3) : *examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements*

L'Ispezione è effettuata secondo criteri di:

- Obiettività, misurando lo stato dell'arte secondo parametri predefiniti,
- Neutralità rispetto alle convinzioni di parte,
- Imparzialità e assenza di conflitti di interesse.

I risultati sono esposti con metriche misurabili e confrontabili rispetto ai massimi obiettivi idealmente raggiungibili dall'organizzazione nel perimetro ispezionato. In tal modo l'organizzazione e i terzi interessati possono utilizzare i risultati dell'Ispezione al fine di valutare la sua maturità in tema di Cyber security secondo criteri oggettivi garantiti da un Organismo di Terza parte affidabile.

1.3 Archivio delle Ispezioni

Tutti i documenti di Ispezione vengono firmati digitalmente e custoditi dal OdI per un periodo non inferiore a 5 anni in un apposito "*Archivio delle Ispezioni*". All'*Archivio* può accedere solo personale autorizzato dal Responsabile del OdI. I documenti presenti nell'Archivio sono considerati come "Confidenziali" secondo il sistema di Classificazione delle Informazioni di Gerico Security Srl.
L'*Archivio delle Ispezioni* permette all'OdI di garantire attività probatoria in merito alle ispezioni effettuate e di gestire eventuali richieste di Attestazione di autenticità e veridicità in merito a Rapporti di ispezione precedentemente prodotti, lecitamente in mano di terze parti interessate. Nessun documento o evidenza prodotto dall'Organizzazione ispezionata viene trattenuto o custodito dall'Organismo di Ispezione e/o dagli Ispettori.

1.4 Richiesta di attestazione veridicità del Rapporto di Ispezione

L'attestazione sullo stato della Cybersecurity dell'Organizzazione risultante dal Rapporto di ispezione, nel formato del Certificato di Ispezione, è usata dall'Organizzazione ispezionata principalmente per dimostrare a soggetti terzi (clienti, partner, Enti regolatori, Pubblica Amministrazione) la propria maturità in termini di Cybersecurity.

L'Organismo di Ispezione garantisce l'autenticità del Certificato di Ispezione e veridicità del suo contenuto attraverso l'applicazione della Firma digitale a tutti i documenti di Ispezione.
Eventuali richieste di attestazione della sua veridicità possono essere richieste da enti terzi a: OdI@gerico-sec.it inviandone la copia e motivandone la necessità.

Qualora l'OdI riceva la richiesta di attestazione da parte di un soggetto terzo, è compito dell'Responsabile Tecnico dell'OdI verificare la fondatezza della richiesta, e quindi verificare l'autenticità della copia del Certificato di ispezione ricevuto tramite il confronto delle firme digitali apposte sul documento.
L'OdI risponde al richiedente entro 10 giorni lavorativi confermando o negando l'attestazione di autenticità della copia del Certificato di Ispezione ricevuto.

2 RIFERIMENTI NORMATIVI

Il presente documento si basa sulle seguenti normative:

- ISO/IEC 17020:2012 “Conformity Assessment – Requirements for the operation of various types of bodies performing inspections”
- ISO17000:2020 “Conformity Assessment – Vocabulary and General principles”
- ILAC P15:05/2020 “Application of ISO/IEC 17020:2012 for Accreditation of Inspection Bodies”
- Accredia - RG-01 – Regolamento per l’accreditamento degli Organismi di Certificazione, Ispezione, Verifica e Convalida – Parte Generale
- Accredia - RG-01-04 – Regolamento per l’accreditamento degli Organismi di Ispezione
- Accredia - RG-09 – Regolamento per l’utilizzo del Marchio Accredia
- ISO/IEC 19011:2018 “Guidelines for auditing management systems”;
- ISO 31000:2018 “Gestione del rischio - Principi e linee guida”;
- D.lgs. 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica;
- Regolamento (UE) 2016/679 in materia di protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali;
- D.lgs. 101/2018 disposizioni per l’adeguamento della normativa nazionale in materia di protezione dei dati personali (D.lgs. 196/2003) alla disciplina europea;
- D.lgs. 81/2008 – Sicurezza sul Lavoro.
- UNI 10459:2017 Attività professionali non regolamentate - Professionista della security - Requisiti di conoscenza, abilità e competenza
- NIST CSF 1.1 16 aprile 2018
- Cini - "Framework Nazionale per la Cybersecurity e la Data Protection" – 2019 - V2.0
- ISACA - "IS Audit/Assurance Program per la Cybersecurity: basato sulla NIST Cybersecurity Framework Audit Program" – 2016
- D.Lgs.65 18/05/2018 “Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione.”
- DPCM 81 del 14/04/2021 “Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all’articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.” Pubblicato in G.U. l’11/06/2021.
- DL.105 del 21/09/2019 “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica” convertito in legge 20/09/20219 con legge n.133 18/11/2019
- IAF MD 4:2018 – IAF Mandatory Document for the use of Information and Communication Technology (ICT) For Auditing/assessment Purposes Issue 2

3 DEFINIZIONI E ACRONIMI

- **ACCREDIA**: Accredia è l'Ente designato dal governo italiano ad attestare la competenza, l'indipendenza e l'imparzialità degli organismi e dei laboratori che verificano la conformità dei beni e dei servizi alle norme. Ogni paese europeo ha il proprio Ente Unico di accreditamento, che opera in linea con quanto stabilito dal Regolamento CE 765/2008 e dalla norma internazionale ISO/IEC 17011. ACCREDIA opera a livello europeo in sede EA (European cooperation for Accreditation) e a livello internazionale in sede IAF (International Accreditation Forum). Quale authority super partes, l'Ente di accreditamento garantisce l'affidabilità dei servizi svolti dagli organismi e dai laboratori, e svolge un servizio di pubblico interesse. In qualità di terza parte indipendente, Accredia garantisce il rispetto delle norme da parte degli organismi e dei laboratori accreditati, e l'affidabilità delle attestazioni di conformità da essi rilasciate sul mercato, svolgendo un servizio a tutela della salute e della sicurezza delle persone e dell'ambiente.
- **Accreditamento:** L'accreditamento attesta il livello di qualità del lavoro di un Organismo (di certificazione e di ispezione), verificando la conformità del suo sistema di gestione e delle sue competenze a requisiti normativi internazionalmente riconosciuti, nonché alle prescrizioni legislative obbligatorie. L'accreditamento è pertanto garanzia di:
  - Imparzialità: rappresentanza di tutte le Parti interessate all'interno dell'Organismo.
  - Indipendenza: gli auditor e i comitati preposti al rilascio della certificazione/rapporto garantiscono l'assenza di conflitti di interesse con l'organizzazione da certificare.
  - Correttezza: le norme europee vietano la prestazione di consulenze sia direttamente che attraverso società collegate.
  - Competenza: l'accreditamento attesta in primo luogo che il personale addetto all'attività di verifica sia culturalmente, tecnicamente e professionalmente qualificato.
- **CDA** - Consiglio di Amministrazione di Gerico Security Srl
- **Committente -** società che ha commissionato l'Ispezione. Potrebbe coincidere con l'Organizzazione ispezionata o essere una terza parte interessata, in tal caso l'Ispezione deve essere concordata e autorizzata dall'Organizzazione.
- **Cybersecurity -** generalmente fa riferimento alla sicurezza informatica al fine di proteggere i sistemi informatici dagli attacchi dall'esterno. In questo documento è associato alla più estesa visione dei processi e tecnologie per la sicurezza delle informazioni gestite, create, archiviate e condivise attraverso sistemi elettronici interconnessi tramite una rete di telecomunicazione locale e/o geografica pubblica e/o privata, con il fine di proteggerne la loro confidenzialità, integrità e disponibilità.

- **Direzione –** La Direzione di Gerico Security Srl è il CDA stesso dell'azienda.
- ***Executive Report –*** *Relazione con la sintesi dello stato della sicurezza cyber dell'organizzazione ispezionata. La relazione va ad esplicitare il contenuto analitico del Rapporto di Ispezione.*
- **GdI – Gruppo di Ispezione**, team di Ispettori Qualificati guidati che effettuano una Ispezione.
- **Ispettore Qualificato -** Ispettore qualificato dall'OdI, e quindi autorizzato, ad effettuare Ispezioni per conto dell'OdI stesso. La qualifica è un processo formale attuato dall'OdI dopo aver valutato con un processo formale le capacità, competenze, conoscenze, e valori etici dell'Ispettore.
- **Ispezione**[3] **-** Esame di un processo, di un servizio, o di una loro progettazione, e determinazione della sua conformità a requisiti specifici o, sulla base di un giudizio professionale, a requisiti generali.
- **Organizzazione** - Ente o società sottoposta ad Ispezione formale.
- **OdI – Organismo di Ispezione**, divisione separata di Gerico Security Srl strutturata ed organizzata al fine di effettuare Ispezioni formali ed imparziali in merito allo stato della sicurezza delle informazioni e cyber di una Organizzazione.
- **Sicurezza delle Informazioni -** tutela dei requisiti di Confidenzialità, Integrità e disponibilità delle informazioni, indipendentemente se siano in formato elettronico o fisico o cartaceo, durante il loro ciclo di vita, dalla loro creazione alla loro distruzione controllata, durante il loro processamento, immagazzinamento e archiviazione, trasmissione e/o comunicazione a terzi tramite strumenti digitali o fisici se non comunicati oralmente.
- **Verifica –** Attività effettuata in ottemperanza al DPCM 81 del 14/04/2021 (Art.8 comma 6) e al DL.105 del 21/09/2019 "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" convertito in legge 20/09/20219 con legge n.133 18/11/2019 (Art.1, comma 6 lett.c)
- **Vulnerability Scan,** attività svolta tramite strumenti automatizzati al fine di identificare l'esistenza di vulnerabilità note nei sistemi e nel software in esecuzione su di essi.

[3] Contestualizzazione della definizione di Ispezione presente nella ISO 17000:2020 (6.3) : *examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements*

4 REQUISITI GENERALI DELL'ORGANISMO DI ISPEZIONE

4.1 Responsabilità dell'Organismo di Ispezione

Avendo la responsabilità di garantire l'esecuzione del processo di Ispezione nella sua interezza, secondo criteri di imparzialità e completezza, l'Organismo di Ispezione:

- adotta un modello che garantisce un formale processo di Ispezione sulla sicurezza delle informazioni e cyber con caratteristiche tali da poter essere valutato affidabile ed essere riconosciuto da soggetti terzi,
- garantisce la completa esecuzione della Ispezione sul perimetro definito contrattualmente con il Committente,
- valuta adeguatamente tempi e modi dell'Ispezione al fine di garantirne la completa esecuzione,
- garantisce la competenza, professionalità e valori etici degli Ispettori e di tutto il personale dell'OdI,
- garantisce la tutela degli interessi dell'Organizzazione ispezionata, in termini di Confidenzialità in merito ai suoi processi, informazioni, conoscenze, strategie e quant'altro dovesse essere conosciuto durante l'attività ispettiva,
- garantisce le necessità dell'Organizzazione ispezionata in termini di minor impegno e disturbo possibile alle attività operative durante l'Ispezione,
- evita di cagionare danni o di aumentare i rischi per l'Organizzazione ispezionata,
- adotta un processo di custodia nel tempo dei risultati delle Ispezioni e di tutta la documentazione prodotta affinché sia, all'interno di un lasso di tempo definito, sempre dimostrabile l'esecuzione ed i risultati dell'ispezione

Le visite ispettive svolte dall'OdI di Gerico Security Srl fotografano tramite campionamento la situazione alla data/e dell'Ispezione. Pertanto, l'Organismo di Ispezione non assume nessuna responsabilità nei riguardi delle eventuali non conformità e/o carenze che risultassero rilevabili soltanto con una presenza continuativa e sistematica in sito.

4.2 Imparzialità ed Indipendenza

Gerico Security Srl ha definito e documentato la propria struttura, la propria organizzazione e ha attuato delle misure organizzative in linea con il proprio Codice Etico, al fine di garantire l'imparzialità delle proprie attività ispettive relative alle tematiche di Sicurezza delle Informazioni e Cyber Security. Nello specifico è stato istituito un "Organismo di Ispezione" (OdI) formalmente indipendente, all'interno della struttura organizzativa, in cui la direzione è impegnata a garantire l'imparzialità nelle attività svolte.

Al fine di salvaguardare l'imparzialità, sono prese in considerazione e trattate tutte le potenziali fonti di conflitto di interessi che vengano identificate, sia che risultino dall'interno dell'Organismo di Ispezione, come l'assegnazione di responsabilità al personale, che dalle attività di altre persone, organismi od organizzazioni. Nello specifico, l'OdI prevede un processo di verifica preventiva dei conflitti di interesse nascenti da nuovi potenziali incarichi, sia come ente sia come personale ispettivo. Ove dovessero emergere tali potenziali conflitti di interesse, è prevista la rinuncia motivata all'incarico, da parte del singolo Ispettore o da parte dell'OdI stesso.

L'Organismo di Ispezione agisce in modo imparziale rispetto ai propri Clienti non risentendo di particolari influenze che potrebbero influenzare le risultanze delle attività ispettive. A maggior tutela e salvaguardia dell'imparzialità si evidenzia come le ispezioni vengano effettuate basandosi su una metodologia riconosciuta a livello nazionale ed internazionale, che garantisce completezza e obiettività della ispezione.

4.3 Confidenzialità

Gerico Security Srl ha tra i suoi principi fondanti la garanzia della confidenzialità delle informazioni dei clienti, in quanto reputa che tutte le attività svolte da essa svolte, da e presso i clienti, hanno natura riservata sia con riferimento ai temi ed argomenti trattati, sia alla natura delle attività eseguite e delle informazioni trattate. Pertanto, Gerico Security Srl si assicura che nessuna informazione acquisita direttamente o indirettamente durante l'attività svolta per i propri clienti possa essere utilizzata al di fuori del contesto per cui è stata ottenuta, o che sia utilizzata al fine di ottenere indebiti benefici finanziari o di mercato.

A tal fine Gerico Security Srl si è dotata di un Sistema di Gestione per la Sicurezza delle Informazioni e si è Certificata secondo la norma ISO/IEC 27001:2013 e i principi e le misure di sicurezza in essere per il perimetro certificato sono applicate anche alle attività dell'Organismo di Ispezione. A tal proposito si richiama in particolare la Politica di Sicurezza delle Informazioni aziendale, presente anche sul sito istituzionale, intesa come l'insieme degli obiettivi e delle direttive strategiche volte ad indirizzare la gestione della sicurezza delle informazioni, detenute e trattate dall'Azienda, nonché le risorse ed i processi informatici necessari per la loro elaborazione.

All'interno della Politica per la Sicurezza delle Informazioni sono definiti:

- Gli obiettivi di sicurezza che essa esprime;
- I requisiti di conformità a livello normativo e di adesione volontaria a standard e le migliori pratiche di settore;
- Il modello logico, organizzativo e gestionale definito per garantire la sicurezza delle informazioni;
- I requisiti per la concreta realizzazione degli obiettivi di sicurezza.

Gli obiettivi di sicurezza espressi nella Policy fanno riferimento alla necessità di contenere, entro limiti accettabili predefiniti, il rischio di compromissioni della riservatezza, dell'integrità e della disponibilità delle informazioni aziendali e dei clienti.

Sulla base della determinazione del profilo di rischio, in caso di superamento dei limiti di accettabilità definiti dal CDA aziendale, la metodologia di analisi e gestione del rischio relativa alle informazioni adottato in Gerico Security prevede l'individuazione delle opportune misure di trattamento al fine di ridurre i rischi entro i limiti di accettabilità costruendo un sistema di contromisure tale da non poter essere eluso se non intenzionalmente. Tali contromisure sono distribuite su diversi livelli, così che un'eventuale debolezza o fallimento di una contromisura sia bilanciato dalla presenza di ulteriori contromisure, anche di diversa natura, per consentire un'adeguata protezione dell'intero sistema ("difesa in profondità").

In particolare:

- La tutela della riservatezza deve attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle informazioni o la diffusione non controllata delle stesse;
- La tutela dell'integrità deve attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
- La tutela della disponibilità deve attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse in tempi utili al compimento della propria missione.

L'insieme di tali interventi si configura come un processo continuo di identificazione, analisi e valutazione dei rischi, nonché di selezione delle migliori strategie di prevenzione e gestione degli stessi, volto a consentire il governo complessivo della sicurezza delle informazioni di Gerico Security Srl.

Infine, i collaboratori dell'azienda e gli Ispettori, qualificati o in qualifica, sono e sensibilizzati e contrattualmente vincolati a mantenere riservate, integre e disponibili le informazioni riguardanti i clienti, le ispezioni e l'OdI stesso.

4.5 Politica del Sistema di Gestione dell'Organismo di Ispezione

Il CDA di Gerico Security Srl ha stabilito di dotare l'Organismo di Ispezione di un Sistema di Gestione per le attività Ispettive. Il CDA ha stabilito, documentato e mantiene la politica dell'Organismo di ispezione che include gli obiettivi per il conseguimento degli scopi della norma ISO 17020:2012 e assicura che la politica sia riconosciuta e attuati a tutti i livelli dell'organizzazione dell'Organismo di ispezione. In particolare:

Il CDA di Gerico Security Srl, consapevole di quanto sia importante erogare i propri servizi nel rispetto dei requisiti di legge e delle aspettative del Cliente, intende promuovere la realizzazione di un Sistema di Gestione per le attività ispettive e impegnarsi al miglioramento continuo della sua efficacia attraverso la periodica individuazione di obiettivi quantificati e verificabili finalizzati alla soddisfazione del Cliente, all'imparzialità e qualità delle ispezioni effettuate.

A tal fine, la Direzione stabilisce la presente politica con i seguenti obiettivi:

- *mantenere la positiva immagine di azienda affidabile e competente conservando nel tempo i rapporti di fiducia con il cliente;*
- *rispettare i requisiti legali, regolamentari e contrattuali*
- *diffondere a tutto il personale la necessaria formazione e informazione;*
- *verificare la rispondenza dei servizi offerti con i requisiti di settore e del cliente e misurarne la soddisfazione;*
- *garantire l'imparzialità dell'Organismo di Ispezione*
- *mantenere riservate tutte le informazioni elaborate durante le ispezioni*
- *mantenere l'eticità nello svolgimento delle ispezioni di sicurezza*
- *garantire il miglioramento continuo delle prestazioni del Sistema di Gestione per le attività ispettive riducendo ogni forma di rischio.*

La Direzione si impegna a comunicare la politica dell'Organismo di ispezione a tutte le parti e a renderla disponibile come informazione documentata. Il Management si impegna a altresì monitorare e revisionare periodicamente tutte le attività, i processi ed i risultati al fine di raggiungere il livello di miglioramento atteso.

La Direzione si impegna a garantire e mantenere nel tempo l'indipendenza dell'Organismo di Ispezione e l'imparzialità di giudizio nei confronti delle Organizzazioni ispezionate.

La Direzione nomina un Responsabile per il Sistema di Gestione che opera per mantenere l'efficacia del SG nel tempo.

4.6 Metodologia di ispezione e procedure

L'Organismo di ispezione ha definito ed utilizza una metodologia formale di ispezione atta a garantire:

- Completezza di valutazione
- Uniformità di giudizio
- Equità di giudizio

La metodologia si ispira sulle migliori partiche del settore al fine di rispondere ai criteri di completezza e rigore dottrinale, ma al contempo garantisce neutralità rispetto ad ambiti di certificazione in merito alla sicurezza delle informazioni e alla cybersecurity in modo da garantire valutazioni non influenzate da giudizi di conformità da soggetti terzi.

Al fine di garantire uniformità ed equità di giudizio la valutazione di singoli aspetti di sicurezza vengono valutati in base a criteri oggettivabili e confrontabili nel tempo.
L'esito dell'Ispezione permette:

- Una valutazione complessiva della maturità e capacità dell'Organizzazione Ispezionata di garantire la sicurezza delle informazioni e cyber
- Una misurazione oggettiva dello stato della sicurezza
- La confrontabilità dei livelli di maturità della sicurezza dell'Organizzazione nel tempo e nei confronti di altre Organizzazioni.

La metodologia di Ispezione è strutturata e formalizzata. Eventuali cambiamenti alla metodologia devono essere basati su rigidi criteri di necessità ed opportunità, quali evoluzioni normative o degli standard di riferimento.
Qualora siano inseriti cambiamenti nella metodologia vengono verificati gli eventuali scostamenti nei risultati rispetto alla versione precedente, e studiate le necessarie misure atte a correggere tali scostamenti. Ove non sia possibile agire per evitare scostamenti nei giudizi, viene comunicato formalmente in caso di richiesta di attestazione le differenze di giudizio tra le successive versioni della metodologia.

L'Organismo di Ispezione regola l'intero processo di ispezione definendo la procedura operativa a cui il Responsabile Tecnico dell'OdI e gli Ispettori si conformano a tali regole per le attività ispettive e le attività correlate.
Il processo inizia con la valutazione dei requisiti di imparzialità e la contrattualizzazione dell'incarico, evolve con le attività ispettive e si conclude con l'archiviazione dei documenti relativi alla ispezione. Le Ispezioni avvengono secondo modalità standard stabilite, secondo una pianificazione concordata con l'Organizzazione ispezionata. L'Ispezione è effettuata e gestita da un uno o più Ispettori sotto la responsabilità finale dell'Responsabile Tecnico dell'OdI che ne firma le risultanze.

4.7 Ispettori Qualificati

Gli Ispettori dell'Organismo di Ispezione possono eseguire ispezioni per conto dell'OdI solo se regolarmente Qualificati dall'OdI secondo procedure formali e devono garantire:

- rispetto di tutte le leggi, regolamenti, provvedimenti amministrativi e in generale delle disposizioni normative applicabili, astenendosi dal compimento di atti illeciti, non conformi al comune senso di rettitudine e al comune senso dell'onore e della dignità
- comportamento irreprensibile, richiedendo in buona fede solo le informazioni necessarie alla propria attività, che mai verranno utilizzate per vantaggio personale o a fine di danneggiare l'organizzazione ispezionata
- rispetto dell'Organizzazione ispezionata, del suo personale, della sua missione e di tutte le parti interessate
- diligenza e qualità nell'ispezione, indirizzando la propria attività ai più elevati standard di ispezione e rispettando gli impegni presi
- confidenzialità: ogni informazione viene acquisita al solo fine dell'ispezione; nulla di quello che viene acquisito verrà utilizzato per fini diversi, o comunicato al di fuori dell'Organizzazione
- imparzialità di giudizio: ogni decisione e valutazione è adottata a prescindere dell'Organizzazione ispezionata, del suo settore merceologico, paese di appartenenza, politica aziendale, stile di gestione, o composizione del personale in termini di età, sesso, razza, credo politico o religioso
- uniformità di giudizio in presenza di situazioni uguali o equivalenti in ispezioni differenti, sia presso la stessa Organizzazione sia in riferimento a differenti organizzazioni.

L'Organizzazione Ispezionata, prima dell'inizio dell'Ispezione ed entro 1 settimana lavorativa dalla ricezione della comunicazione di designazione, ha la facoltà di chiedere la sostituzione di un Ispettore se tale richiesta è motivata. Ove l'Ispezione venga contrattualizzata a ridosso dell'effettuazione attività, l'Organizzazione Ispezionata rinuncia automaticamente alla ricusazione dell'Ispettore.

4.8 Gestione delle evidenze

Gli Ispettori garantiscono la massima diligenza nel trattare le evidenze di volta in volta richieste nelle ispezioni. Non vengono richieste più evidenze dello stretto necessario.
Gli Ispettori garantiscono massima confidenzialità delle informazioni acquisite tramite l'analisi delle evidenze fornite dall'Organizzazione ispezionata.
Per quanto possibile le evidenze restano nel perimetro dell'Organizzazione Ispezionata, e se in formato digitale ne viene richiesta la condivisione in sola lettura senza salvarne copia in locale.
Eventuali evidenze nella disponibilità vengono riconsegnate all'Organizzazione ispezionata o distrutte.

4.9 Registrazione delle Ispezioni

Tutte le informazioni raccolte dagli ispettori durante le ispezioni che permettono di definire o ricostruire la valutazione vengono registrate negli appositi campi della Checklist utilizzata per l'attività ispettiva. La Checklist firmata dell'Responsabile Tecnico del OdI, è archiviata a fini probatori qualora vi siano ricorsi o altre necessità nell'Archivio delle Ispezioni assieme a tutte le altre informazioni attinenti all'ispezione.

4.10 Attività di controllo da parte degli Organismi di Accreditamento

Quale Organismo di Ispezione ISO/IEC17020 accreditato, Gerico Security Srl è soggetto ad attività di controllo da parte di Organismi di Accreditamento[4], i quali conducono verifiche ispettive presso la sede dell'Organismo di Ispezione, sia accompagnando gli Ispettori dell'Organismo stesso nel corso di alcune verifiche ispettive presso le organizzazioni, per verificare in campo l'adeguatezza e la corretta applicazione delle procedure, nonché il comportamento degli stessi Ispettori. In sostanza la presenza degli Ispettori dell'Organismo di Accreditamento presso l'organizzazione ispezionata ha lo scopo di verificare l'adeguatezza del comportamento dell'Organismo di Ispezione e di assicurare in merito all'uniformità del giudizio professionale espresso.
ACCREDIA si assume direttamente la responsabilità sui loro incaricati in accompagnamento all'Organismo di Ispezione. È facoltà dell'Organizzazione Ispezionata chiedere ad Accredia la sottoscrizione di uno specifico accordo di riservatezza.
Il mancato accesso agli Ispettori Accredia, non adeguatamente giustificato, può determinare il blocco della attività Ispettiva presso l'Organizzazione Ispezionata inadempiente.

ACCREDIA può anche verificare autonomamente le informazioni ricevute dall'Organismo di Ispezione di Gerico Security Srl, per esempio contattando gli Ispettori o una Organizzazione Ispezionata, durante o anche dopo l'Ispezione.

[4] In Italia l'Organismo di Accreditamento è ACCREDIA

5 RESPONSABILITA' DEL CLIENTE

5.1 Responsabilità dell'Organizzazione Ispezionata

L'Organizzazione Ispezionata deve assicurare al Gruppo di Ispezione (GdI) l'esecuzione ordinata e completa delle loro attività, ovvero:

- concordando il Piano di Ispezione definitivo con il GdI, identificando luoghi, processi, tecnologie e referenti nel perimetro delle attività Ispettive,
- garantendo fattiva collaborazione con il GdI, assegnando un referente interno che funga da punto di contatto per qualsiasi necessità emerga prima e durante l'ispezione
- evitando di porre ostacoli o qualsiasi situazione di contrasto con gli Ispettori per l'ordinato svolgimento del loro incarico,
- garantendo l'accesso alle aree sottoposte ad ispezione come da Piano di ispezione,
- assicurando il personale di supporto per l'accesso ai sistemi e tecnologie da ispezionare,
- assicurando l'accesso ai documenti, ai sistemi ed informazioni necessarie alla Ispezione, come richiesto dal GdI
- assicurando tempi e luoghi idonei per poter intervistare i referenti dei processi in perimetro,
- accettando che tutta la documentazione prodotta durante l'Ispezione sia archiviata dall'OdI.
- accettazione della eventuale partecipazione degli ispettori ACCREDIA alle verifiche in campo, in qualità di osservatore.
- accettazione di rispondere alle eventuali domande poste da ACCREDIA in merito alle modalità di svolgimento delle attività dell'Organismo di Ispezione di Gerico Security Srl.

Qualora l'Organizzazione Ispezionata non sia il Committente dell'ispezione, l'Organizzazione deve:

- concordare con il Committente l'attività ispettiva, tempi e perimetro,
- autorizzare formalmente l'OdI ad eseguire l'Ispezione e a consegnare al Committente il Rapporto di ispezione, nella versione di Rapporto Pubblico.

5.2 Responsabilità del Committente terzo

Qualora l'Ispezione sia richiesta da un differente ente o società rispetto all'Organizzazione da ispezionare, il Committente deve:

- concordare con l'Organizzazione da ispezionare l'Ispezione al fine di autorizzare l'OdI ad effettuare l'attività, concordando tempi e perimetro dell'attività,

- garantire all'OdI che l'Ispezione non avvenga in contrasto con la volontà dell'Organizzazione
- supportare l'OdI e l'Organizzazione al fine di identificare il perimetro dell'ispezione,
- accettare quale risultato dell'attività il Rapporto di ispezione nella forma di Rapporto Pubblico, evitando di richiedere all'OdI i documenti di dettaglio ad uso esclusivo dell'organizzazione e destinati all'archiviazione presso l'OdI.

6 PROCESSO DI ISPEZIONE

Il processo Ispettivo si compone di quattro attività successive, descritte nei sotto paragrafi seguenti:

6.1 Valutazione imparzialità a seguito di richiesta di Ispezione

Alla ricezione di una richiesta di ispezione, il Responsabile Tecnico dell'OdI si accerta che l'ispezione richiesta non risulti in conflitto di interesse con eventuali precedenti attività. Qualora emergano potenziali conflitti di interesse, non potendo garantire l'imparzialità gli è fatto obbligo di rinunciare all'incarico proposto.

6.2 Contrattualizzazione di una Ispezione

L'Ispezione sulla sicurezza delle informazioni e cyber, così come previsto all'interno dello standard ISO/IEC 17020 al punto 4.1.6 può essere di:

a) indirizzata alla propria organizzazione, e in tal caso il Committente e l'Organizzazione ispezionata coincidono,
b) essere commissionata da un Committente per effettuare una Ispezione presso un altro soggetto, l'Organizzazione ispezionata.

Nel caso in cui un Committente richieda una attività ispettiva presso un soggetto terzo, quest'ultimo deve concordare ed autorizzare esplicitamente l'Ispezione[5].
A tal fine il Committente deve obbligatoriamente consegnare all'OdI il Modulo di Autorizzazione all'Ispezione conto terzi, debitamente compilata, datata e firmata dall'Organizzazione da ispezionare, **prima che l'OdI possa accettare e firmare l'incarico**.

L'attività ispettiva viene contrattualizzata con il Committente avendo cura di identificare compiutamente il perimetro dell'ispezione in termini di:

a) Sedi da ispezionare
b) Processi pertinenti l'ispezione
c) Contesto tecnologico
d) Tempi di esecuzione

[5] Una Ispezione presso un soggetto terzo può avvenire ad esempio quando l'organizzazione ispezionata ha specifici vincoli contrattuali in materia di cybersecurity con il Committente.

e) Modalità di Ispezione (parti in presenza, in videocall, in backoffice)
f) Referente dell'Organizzazione e del Committente.
g) Eventuali permessi o altri aspetti logistici necessari all'GdI
h) Perimetro tecnologico per l'effettuazione di un Vulnerability Scan

6.3 Effettuazione dell'Ispezione

L'ispezione è una attività formale accompagnata da attività preparatorie e attività di chiusura nei limiti di quanto previsto dal Contratto con il Committente. Nel rispetto delle differenze, l'Organismo di Ispezione di Gerico Security Srl struttura le modalità di Ispezione in linea con la ISO19011:2018 adeguatamente contestualizzata per le attività di ispezione.

Il Responsabile Tecnico dell'OdI identifica gli Ispettori che condurranno l'attività ispettiva in base alla dimensione e specificità della attività contrattualizzata, verificando con loro la presenza di eventuali conflitti di interesse, e comunica i loro nominativi all'Organizzazione Ispezionata. L'Organizzazione ispezionata può nell'arco di 1 settimana lavorativa può chiedere la sostituzione di uno o più ispettori se adeguatamente motivato. Ove i tempi di accettazione formale del contratto siano a ridosso dell''ispezione, l'Organizzazione Ispezionata rinuncia alla possibilità di ricusare l'ispettore.
Il Gruppo di Ispezione definisce e concorda il Piano di Ispezione con il referente dell'Organizzazione Ispezionata, identificando luoghi, processi, tecnologie e referenti nel perimetro delle attività Ispettive.
Le attività preparatorie si concludono con il Responsabile Tecnico dell'OdI, che analizzando il Contratto e seguendo le indicazioni del Committente, garantisce al GdI tutti gli adempimenti di legge e eventuali permessi per operare presso l'Organizzazione Ispezionata.

L'Ispezione viene svolta su tutti i siti, processi e sistemi in perimetro, utilizzando la specifica "Checklist di Ispezione dell'OdI".

I processi e misure di sicurezza dell'organizzazione vengono valutati in base alle Pratiche di sicurezza presenti nella Checklist, valutandone preliminarmente la loro applicabilità al contesto ispezionato (qualora non applicabili vengono eliminate dalla valutazione e non influiscono sulla valutazione complessiva dell'Organizzazione in termini di Score nel Rapporto di ispezione).

Per ogni pratica di sicurezza, come presente nella Checklist, viene valutata la sua consistenza e la sua maturità all'interno dell'Organizzazione Ispezionata in base a:

- La Maturità delle pratiche di sicurezza
- La consistenza di implementazione delle pratiche di sicurezza

La profondità di ispezione per singola Pratica dipende dalla complessità della pratica o della modalità di implementazione della misura di sicurezza, ed è volta a rimuovere eventuali dubbi all'ispettore. Qualora non vi siano dubbi in merito alla modalità di implementazione della pratica di sicurezza, l'Ispettore deve procedere senza indugio alla Pratica successiva non richiedendo all'Organizzazione ispezionata più informazioni del necessario.
Tramite le interviste e ispezioni presso i siti dell'Organizzazione vengono verificate la effettiva implementazione delle pratiche di sicurezza.

Inoltre, a conclusione della valutazione di tutte le pratiche di sicurezza applicabili, viene determinata la maturità di gestione dei rischi di cybersecurity sulla base delle risultanze presenti nel relativo foglio della Checklist ottenendo uno score complessivo come da Cap.9.
In parallelo alla valutazione dei processi di gestione delle vulnerabilità, viene anche valutata la corrente gestione delle vulnerabilità sui sistemi informatici attraverso un Vulnerability Scan, sul perimetro esterno, effettuato tramite uno strumento automatizzato[6].

6.4 Chiusura dell'Ispezione

Terminata la valutazione di tutte le Pratiche di sicurezza presenti nella Checklist, e valutato il livello di Maturità nella Gestione di Rischi, il Gruppo di Ispezione presenta al Referente dell'Organizzazione ispezionata i risultati in sintesi dell'Ispezione che possono evidenziale eventuali criticità.

L'Organizzazione ispezionata ha tempo 2 giorni lavorativi successivi all'incontro di chiusura per fornire evidenze[7] che chiariscano le pratiche di sicurezza a cui fanno riferimento tali criticità.
Il Rapporto di Ispezione potrà eventualmente contenere nella apposita sezione eventuali note integrative sintetiche del Responsabile di Ispezione in merito alle modalità di svolgimento dell'attività e di eventuali criticità e/o peculiarità in merito all'Ispezione effettuata.

Chiusa l'Ispezione, il Rapporto e tutta la documentazione afferente all'ispezione viene presa in carico dal Responsabile Tecnico dell'OdI, il quale ne analizza la congruità e qualità, dichiarando formalmente chiusa l'Ispezione. Il Responsabile Tecnico firma digitalmente e archivia tutta la documentazione dell'ispezione presso *l'Archivio delle Ispezioni* dell'OdI quale documentazione ufficiale.

[6] Il Vulnerability Scan viene effettuato sul perimetro esterno attraverso lo strumento in dotazione all'OdI e previsto dalla Procedura Operativa.
[7] Si fa presente che non saranno accettate evidenze che corrispondono ad attività correttive poste in essere a seguito della visita ispettiva.

7 RAPPORTI DI ISPEZIONE E DOCUMENTAZIONE RELATIVA

I rapporti di ispezioni sono in forma tale da permettere una chiara identificazione e misurazione dello stato della sicurezza dell'Organizzazione ispezionata. Al contempo l'associazione del Certificato al Rapporto deve garantire:

a) All'Organizzazione ispezionata la comprensione dello stato complessivo, avendo una visione dei punti di forza e di debolezza
b) Alle terze parti interessate lo stato di sicurezza dell'Organizzazione ispezionata senza accedere a informazioni confidenziali di quest'ultima

I risultati dell'ispezione vengono forniti tramite un Rapporto di ispezione a cui è associato un Certificato di Ispezione, in cui:

1) **Rapporto di Ispezione**[8], che illustri nel dettaglio la maturità dei processi dell'organizzazione in merito alla sicurezza delle informazioni e cyber;
2) **Certificato di Ispezione**[9], associato al Rapporto di Ispezione che indichi esclusivamente la valutazione generale della maturità dell'Organizzazione Ispezionata in merito alla sicurezza delle informazioni e cyber, utile per una distribuzione a terzi.
3) ***Executive Report,*** *Relazione con la sintesi dello stato della sicurezza cyber dell'organizzazione ispezionata. La relazione va ad esplicitare in formato testuale il contenuto analitico del Rapporto di Ispezione ai soli fini di una migliore comprensione dei risultati dell'ispezione.*

Eventuali aggiornamenti alla documentazione di ispezione a seguito di ricorso determinano la emissione di documenti con l'identificazione della modifica in termini di nuova edizione. Le versioni precedenti vengono annullate ma non vengono cancellate e vengono mantenute archiviate.

La custodia della documentazione delle ispezioni avviene nello specifico "Archivio delle Ispezioni" e mantenuta per 5 anni.

Tutta la Documentazione condivisa ai fini dell'Ispezione in formato Digitale alla fine delle attività viene cancellata in modalità sicura dai sistemi dell'OdI e quelle prodotte in formato cartaceo riconsegnate all'Organizzazione, o su sua richiesta distrutte.

[8] Il Rapporto di Ispezione è, nell'effettuazione dell'Ispezione sulla Sicurezza delle Informazioni e Cyber, quello definito in ISO/IEC17020:2012 Cap.7.4 punto 7.4.3.
[9] Il Certificato di Ispezione è, nell'attestazione di scoring in merito alla Sicurezza delle Informazioni e Cyber, quello definito in ISO/IEC17020:2012 Cap.7.4 punto 7.4.3.

8 RECLAMI E RICORSI

L'Organismo di Ispezione è strutturato per garantire alle Organizzazioni ispezionate la possibilità di effettuare reclami sul suo e/o sull'operato degli Ispettori, nonché la possibilità di effettuare Ricorsi in merito agli esiti dell'ispezione.

I Reclami, essendo rivolti all'operato stesso dell'OdI, e quindi riguardanti aspetti di etica o qualità dell'attività ispettiva, sono gestiti dalla Direzione aziendale, mentre i Ricorsi, mirati a contestare i risultati di una Ispezione sono gestiti dall'Responsabile Tecnico dell'OdI.

8.1 Reclami

L'Organismo di Ispezione comunica all'Organizzazione ispezionata le modalità di invio di un reclamo formalizzandole nel Contratto di autorizzazione all'attività ispettiva.

In particolare, eventuali reclami possono essere inviati all'indirizzo reclami@gerico-sec.it avendo cura di riportare i dati del reclamante, una descrizione dettagliata del reclamo ed allegando eventualmente i documenti ritenuti utili a supporto dello stesso. L'OdI risponde tramite e-mail al reclamante in merito alla presa in carico del reclamo il prima possibile.

Il reclamo viene gestito direttamente dalla Direzione aziendale, la quale si impegna a fornire al reclamante una risposta via e-mail entro 10 giorni lavorativi.

8.2 Ricorsi in merito ai risultati di una Ispezione

L'Organizzazione ispezionata può esercitare il diritto di contestare particolari contenuti della documentazione finale della Ispezione (intesi come Rapporto e/o Checklist di ispezione) entro 5 giorni lavorativi dalla consegna di tale documentazione da parte dell'OdI, inviando comunicazione motivata a: OdI@gerico-sec.it o tramite PEC a gericosecurity@pec.it indicando i contatti di un referente per la risoluzione della contestazione.

Eventuali divergenze nelle valutazioni vanno motivate e documentate dall'Organizzazione ispezionata tramite evidenze che ne dimostrino la non corretta comprensione da parte del Gruppo di Ispezione. Le evidenze non possono fare riferimento a modifiche poste in essere dall'Organizzazione Ispezionata successivamente all'Ispezione.

Il Responsabile Tecnico dell'OdI contatta il referente indicato nella comunicazione dell'Organizzazione ispezionata entro 5 giorni lavorativi, e fissa una data congrua per la discussione in merito alla contestazione, richiedendo all'organizzazione ispezionata di produrre le evidenze che ne dimostrino la non corretta comprensione da parte del Gruppo di Ispezione.

L'analisi del Ricorso viene effettuata dal Responsabile del Sistema di Gestione per le attività ispettive, in qualità di referente indipendente dalla Ispezione, eventualmente coadiuvato da Ispettori Qualificati sempre estranei all'ispezione in oggetto e non aventi conflitti di interesse relativi all'Organizzazione ispezionata.

L'analisi viene effettuata assieme al referente indicato dall'Organizzazione ispezionata, prevedendo la valutazione della documentazione e le evidenze a supporto della contestazione. Qualora la contestazione sia ritenute giustificata, il Responsabile del Sistema di Gestione per le attività ispettive richiede al Responsabile Tecnico dell'OdI di provvede a:

- annullare la precedente Checklist di ispezione presente in Archivio
- annullare il precedente Rapporto di ispezione (e il Certificato associato)
- correggere la valutazione presente nella "Checklist di ispezione",
- re-emettere tutta la documentazione di Ispezione in base alla nuova valutazione, firmando digitalmente la nuova versione con la data corrente, e inserendo nella "Nota Integrativa" l'indicazione che annulla la versione precedente.

L'OdI risponde alla Organizzazione ispezionata tramite PEC con le risultanze della valutazione effettuata, e ove siano stati corretti i documenti di ispezione, allegandoli alla stessa.

La contestazione viene registrata nell'apposito *Registro dei Reclami*, indicandone tempi, motivazione, e risoluzione. Tutte le evidenze prodotte dalla Organizzazione Ispezionata in formato Digitale al fine della discussione in merito alla contestazione vengono cancellate in modalità sicura dai sistemi dell'OdI e quelle prodotte in formato cartaceo riconsegnate all'originante, o su sua richiesta distrutte.

9 CONDIZIONI GENERALI PER I SERVIZI DI ISPEZIONE

9.1 Contratto di Ispezione

Il Contratto di Ispezione è in formato standard. Eventuali modifiche o alterazioni sono possibili solo per la definizione di specificità nell'ispezione stessa, ad esempio, ove si renda necessario l'espletamento di particolari norme cogenti precedentemente o durante l'attività ispettiva. Tali modifiche devono comunque essere in linea con il Codice Etico di Gerico Security Srl e non creare alterazioni agli obiettivi e principi dell'Ispezione stessa.

Nessuna modifica al contratto sarà ritenuta valida a meno che essa non sia scritta e controfirmata dalle parti. Qualunque condizione o prescrizione che venisse unilateralmente predisposta dal Committente, e che risulti in contrasto con le presenti condizioni, non avrà effetto, a meno che non sia accettata per iscritto dall'Organismo di Ispezione.

9.2 Utilizzo del Marchio

L'uso del marchio di Gerico Security Srl da parte del Committente o dell'Organizzazione Ispezionata è consentito esclusivamente dietro preventiva ed esplicita autorizzazione scritta da parte di Gerico Security Srl. L'utilizzo del marchio deve essere riferito esclusivamente ai perimetri interessati dalle ispezioni effettuate dall'Organismo di Ispezione ed a cui attengono i Rapporti e documenti rilasciati da Gerico Security Srl. La facoltà di utilizzare il marchio Gerico Security Srl non può essere in alcun modo trasferita a terzi dal Committente o dall'Organizzazione Ispezionata. L'utilizzo del marchio di accreditamento ACCREDIA da parte di Gerico Security Srl è svolto in conformità al Regolamento Generale ACCREDIA RG-09 disponibile sul sito ACCREDIA www.accredia.it. In particolare, i Certificati e i Rapporti di Ispezione rilasciati dall'Organismo di Ispezione nell'ambito dello scopo di accreditamento riportano il marchio ACCREDIA. L'uso del marchio ACCREDIA è precluso al cliente.

9.3 Modifiche allo Schema di Ispezione

Qualora vengano apportate modifiche sostanziali alle regole dello schema di ispezione, dovuti alla emissione di una nuova versione della linea guida di riferimento e la conseguente revisione della Checklist di ispezione, l'Organismo di Ispezione ne informa il Committente e l'Organizzazione sottoposta ad Ispezione prendendo in considerazione le eventuali osservazioni da questi presentate. L'allineamento verrà effettuato avendo cura di valutare e gestire opportunamente eventuali scostamenti di Score rispetto alle Ispezioni già effettuate.

L'Organismo di Ispezione provvede a specificare la data di entrata in vigore delle modifiche e a darne pubblicità attraverso il sito WEB istituzionale di Gerico Security Srl.

10 METODOLOGIA DI ISPEZIONE E SCORING FINALE

L'Ispezione di Cybersecurity dell'Organismo di Ispezione di Gerico Security Srl utilizza come base di riferimento una linea guida internazionale di settore, nello specifico il:

- "Framework Nazionale per la Cybersecurity e la Data Protection", meglio conosciuto come "CSF Nazionale" V2.0, che a sua volta è derivato dal
- "CSF – Cyber Security framework" del NIST[10] americano V1.1
- ISACA - "IS Audit/Assurance Program per la Cybersecurity: basato sulla NIST Cybersecurity Framework Audit Program" - 2016

Il CSF, nasce per dare le linee guida di cybersecurity alle Infrastrutture critiche statunitensi, e poi suggerita per tutte le imprese americane. Il CSF Nazionale ha seguito la stessa traccia, e all'inizio è stata proposto quale metodologia per rispondere alle esigenze delle infrastrutture critiche italiane in merito alla Direttiva UE 2016/1148 NIS, per poi essere raccomandata quale metodologia di implementazione della Cybersecurity per qualsiasi azienda nazionale, indipendentemente dalla loro dimensione o settore.
Al CSF Nazionale[11] sono stati in particolare aggiunti specifici controlli in merito alla Data Protection dei dati personali, non presenti nella versione americana.

L'utilizzo del CSF garantisce che la completezza di valutazione degli aspetti di Information & Cyber security secondo una *best practice* nata per guidare le imprese nella implementazione della Cybersecurity e risulta NEUTRALE agli aspetti di certificazione di terza parte.

Il CSF enumera una serie di controlli di Cybersecurity suddivisi per Function, ovvero momenti del ciclo di un complessivo processo continuo di sicurezza. Tali controlli non necessariamente sono tutti applicabili, in quanto dipendono dalla dimensione e contesto dell'organizzazione. La Checklist di ispezione, quindi, tiene in considerazione tale premessa, prevedendo che i controlli in checklist possano essere dichiarati non applicabili.

Al fine di Garantire un processo valutativo equo ed uniforme, l'OdI ha implementato nella Checklist di ispezione una serie di meccanismi automatici che permettono di dare uno scoring numerico quanto più possibile oggettivo in merito alla valutazione effettuata dall'Ispettore.

[10] Cybersecurity Framework | NIST (www.nist.gov/cyberframework)
[11] Framework Nazionale per la Cyber Security e la Data Protection (www.cybersecurityframework.it)

10.1 Risultati dell'Ispezione

10.1.1 Score presentati nel Rapporto in formato di Rapporto pubblico

Il Rapporto di Ispezione e il Certificato riporta lo Score finale in merito ai seguenti elementi della sicurezza delle informazioni e cyber:

- Adeguatezza delle misure e pratiche di sicurezza
- Grado di maturità nella gestione delle pratiche di sicurezza
- Gestione delle vulnerabilità di sicurezza dei sistemi ed applicativi[12]

Questi valori vengono riportati in forma di "Score" percentuale e attraverso grafici che ne permettano una immediata comprensione.

10.1.2 Calcolo dello Score

Il numero di controlli di cyber security parte dal numero massimo presente nel CSF di 117 controlli. Tuttavia, il CSF è una linea guida valida a prescindere dal tipo o dimensione dell'organizzazione, dal suo contesto operativo o del perimetro ispezionato. La linea guida indica che i controlli vanno scelti in base all'organizzazione, in quanto alcuni potrebbero essere non applicabili.
Lo score viene quindi calcolato solo sui controlli applicabili in base a quanto valutato dall'ispettore, prevedendo la somma dei risultati di tutti i controlli applicabili.

Dato che lo Score massimo è dipendente dal numero di controlli applicabili in fase di ispezione, nel Rapporto di Ispezione lo **Score di riferimento è illustrato in forma percentuale** rispetto al valore massimo teorico realizzabile:

Percentuale Score	**0,00%**

[12] La valutazione degli aspetti di gestione delle vulnerabilità si completa con l'effettuazione del Vulnerability Scan che permette di valutare compiutamente il processo in essere presso l'organizzazione. Non verranno fornite informazioni relative alla risoluzione delle problematiche identificate dal sistema automatico

10.2 Valutazione dei livelli risultanti dello Score

I valori di Score presenti nel Rapporto e nel Certificato di Ispezione sono illustrati in forma percentuale, in cui **il 100% è da considerare un valore ideale**, realisticamente di difficile raggiungimento, in quanto la sicurezza delle informazioni e cyber è un processo in continuo mutamento, sia in reazione alle minacce e rischi, sia in relazione alle tecnologie e processi di contrasto a tali minacce e rischi. La presente tabella illustra in classi come dovrebbero essere considerati gli Score ottenuti:

Classe di Score		Valutazione
>=90%	**Alta**	L'Organizzazione dispone di un elevato grado di maturità e di controllo degli aspetti rilevanti alla Sicurezza delle Informazioni e Cyber. Ha definito processi e controlli in linea con le migliori pratiche internazionali e adotta in sistema di controllo che tali pratiche siano coerenti nel tempo.
>=75%	**Medio-Alta**	L'Organizzazione dispone di un buon grado di maturità e di controllo degli aspetti rilevanti alla Sicurezza delle Informazioni e Cyber. Tuttavia, presenta alcune carenze e alcuni aspetti deviano rispetto alle migliori pratiche internazionali.
>=50%	**Medio-Bassa**	L'Organizzazione ha approcciato ed implementato misure per la Sicurezza delle Informazioni e Cyber. Tuttavia, l'approccio non adeguatamente strutturato fa emergere carenze e deviazioni significative rispetto alle migliori pratiche internazionali.
<50%	**Bassa**	L'Organizzazione evidenzia significative carenze in merito alla Sicurezza delle Informazioni e Cyber.

<fine documento>