LL-C
Certification

2a fase di audit

F 43 S

RAPPORTO DELLA VERIFICA DI CERTIFICAZIONE NO. 3914919
ISO/IEC 27001:2013

redatto il giovedì 22 giugno 2023

presso

Excellence Innovation S.R.L.

DATI GENERALI CLIENTE

Excellence Innovation S.R.L.

Via Vittor Pisani, 7
20124 Milano (MI)

P. IVA 08741540960 IT08741540960

Riferimento

Michele Celeghini (Rappresentante dell'impresa), e-mail: celeghini@exin.digital, gruppoexcellence.com

Il prodotto o servizio principale dell'azienda di cui si valuta il Sistema di Gestione per richiederne la Certificazione è il seguente

Progettazione, sviluppo, installazione e assistenza di sistemi informativi e consulenze tecniche.

Codice NACE corrispondente	99.98
Numero di dipendenti dell'area certificata	9
Numero di sedi operative oltre la sede legale dell'organizzazione	1
Processi particolari	
I processi certificati sono garantiti da	tutti i dipendenti dell'azienda, senza eccezioni
Numero di turni	1,00

DATI SUL PROCEDIMENTO DI CERTIFICAZIONE

Standard richiesto per la certificazione	ISO/IEC 27001:2013
Data della verifica	10/06/2023 08:00:00 - 22/06/2023 15:00:00
Svolgimento della verifica presso	Sede amministrativa e filiali
Coordinatore Audit e Lead Auditor	Paolini Pietro (ISO/IEC 27001:2013)
Altri partecipanti all'audit (e rispettivi ruoli)	Tomaso Brambilla (project manager) Michele Celeghini (direttore generale)
Data del Piano di Verifica	lunedì 5 giugno 2023
Totale durata della verifica (in loco)	3,50 (1,96)
Il piano di verifica è stato modificato dopo la riunione iniziale	NO
Problemi significativi nella programmazione di audit o nel sistema di gestione dell'azienda	NO
Coinvolgimento consulente/i a supporto del Sistema di Gestione	-
Lingua in cui e stata svolta la verifica	Italiano

1. AMBITO DELLA VERIFICA

Criteri di audit

I criteri di audit sono i requisiti dello standard e dei processi stabiliti, nonché la documentazione del sistema di gestione dell'organizzazione. Lo scopo dell'audit è di confermare la conformità del sistema di gestione del cliente con i criteri di audit e ne determinano la capacità di garantire il soddisfacimento dei requisiti legali e di altro tipo da parte dell'organizzazione. Inoltre, l'obiettivo è determinare se l'efficacia del sistema di gestione rende possibile raggiungere gli obiettivi preposti e identificare potenziali aree di miglioramento.

Descrizione dell'organizzazione certificata e della sua attività

Dettagli dell'azienda, infrastruttura, luoghi di lavoro e sedi distaccate, descrizione dell'organigramma

Excellence è un gruppo multi-boutique formato da più società con diversa specializzazione.
L'ufficio di sviluppo software, di una superficie complessiva di 250mq circa.
Vi sono 2 filiali: la sede principale e una sede operativa.
La sede principale è sede legale senza processi operativi; tutte le attività sono svolte nella sede operativa.

Attrezzatura produttiva o attivita di supporto per servizi

Ogni ufficio è dotato di scrivania, computer, telefono e spazio per riunioni private o confidenziali. Ci sono due spazi aperti, detti open space. Non sono presenti server di elaborazione dati negli uffici, i dati
sono in cloud presso OVH e AWS.

Descrizione del prodotto o del servizio principale

Progettazione, sviluppo, installazione e assistenza di sistemi informativi e consulenze tecniche.

Risorse Umane

Vi sono circa 12 addetti medi annui e gran parte del personale ha una notevole esperienza e specializzazione nei servizi erogati.
Gli addetti FTE medi annui sono 9.

Ambito della certificazione

Progettazione, sviluppo, installazione e assistenza di sistemi informativi e consulenze tecniche.

Aree escluse dalla certificazione

nessuna

Obiettivi di audit

Obiettivi di audit, laddove metodologicamente possibile 1) confermare la conformità del sistema di gestione del cliente con criteri di audit, 2) determinare la capacità del sistema di gestione di garantire che l'organizzazione soddisfi i requisiti statutari, normativi e contrattuali applicabili, e 3) raggiungere gli obiettivi specificati, in quanto il sistema di gestione può identificare aree per potenziali miglioramenti, tra cui revisione della direzione e audit interni - Sono stati soddisfatti.

Procedura della certificazione

Dichiarazione di non responsabilità

L'auditing si basa su un processo di campionamento delle informazioni disponibili e di conseguenza vi sarà sempre un elemento di incertezza presente nelle prove di auditing che può riflettersi nei risultati dell'audit. Coloro che fanno affidamento o agiscono in base ai risultati e alle conclusioni dell'audit dovrebbero tener conto di questa incertezza.

Partecipanti alle riunioni iniziali e finali

Tomaso Brambilla (project manager) Michele Celeghini (direttore generale)

Metodi di verifica

L'audit è stato eseguito in remoto seguendo il metodo CAAT / ICT 30 %
Tipo di audit: conferenze telefoniche con i rappresentanti dell'organizzazione, comunicazione e-mail
Il metodo CAAT/ICT di audit da remoto è stato utilizzato efficacemente utilizzando gli strumenti elencati di cui sopra - soddisfatto.
Effettuata verifica a campione dei documenti e delle attività, assistenza a processi operativi: gestione della sicurezza delle informazioni di cui alle commesse dei cliente WFCrediti e Banca Immobiliare.

Volume delle vendite, prodotti, ordini, servizi, a seconda dei casi

Fatturato medio annuo: l'azienda è in crescita: il valore produzione 2020: € 777.779, 2021: € 854.425, 2022 € 1,1 mln circa.
Numero medio commesse annue gestite: 12 commesse annue più 10 contratti continuativi di erogazione e manutenzione.

Descrizione del campionamento e statistiche

Commesse WFCrediti e Banca Immobiliare:
Testbook compilati dall'utente ad ogni rilascio in produzione del software commissionato es.:
- 20221115_Testbook_MS1 _ EB_v.3_esiti per Testbook Task MS1 cliente Banca Euromobiliare, Collaudo del 07/11/2022, Produzione del 20/11/2022
- UAT wf crediti del 06 06 23.v1, Test Book cliente WF Crediti - Evolutive Maggio 2023 Collaudo del 05/06/2023 Produzione del 09/06/2023
- Report Analisi relativo al Progetto WF Crediti, ver. 1.9 del 05.04.2022

Cambiamenti significativi del sistema di gestione e problemi irrisolti dell'organizzazione verificatisi dal precedente audit

-

LOGO of the Certification Body and certification reference

è usato in maniera comune, non è fuorviante o inconsistente con i termini delle condizioni commerciali

2. DESCRIZIONE DEL SISTEMA E MATRICE DI CONFORMITA ISO/IEC 27001:2013

Descrizione del sistema

Contesto dell'organizzazione - ambito del business e parti interessate

Le aspettative delle parti interessate interne ed esterne sono descritte nel manuale del SG e nel documento Analisi del Contesto ed analisi dei Rischi in conformità ai requisiti della norma UNI CEI EN ISO/IEC 27001:2017 agg. al 20.06.2023.

L'organizzazione Azienda ha adottato e implementato la metodologia "Privacy Impact Analysis" (PIA) non solo per la gestione della privacy, ma estendendola a tutte le linee di sviluppo e servizio considerate critiche.

Ambito/Scopo dell'ISMS

Il campo di applicazione del sistema di gestione risulta definito e conservato come informazione documentata all'interno del documento Politica e campo d'applicazione del 20.06.2023, senza esclusioni

Progettazione, sviluppo, installazione e assistenza di sistemi informativi e consulenze tecniche.

Impostazioni ISMS

Aggiornato il documento di analisi dei rischi, definiti i criteri, per i quali l'analisi effettuata permette di individuare aree e/o aspetti critici per le quali opportunamente valutate (con criteri definiti) permette di attivare azioni al fine di ridurre il rischio di accadimento fino a ridurlo ad un rischio ritenuto accettabile.

Leadership, ruoli, impegno e politiche

Organigramma aziendale definito sul moduloRev. 1 del 20.06.2023
- CEO: Stefano Spalletta
- Direttore Generale: Michele Celeghini
- Responsabile sistema di gestione delle informazioni RGSI: Michele Celeghini (ad interim)
- Amministratore di sistema (esterno): Rinaldo Cavalieri
- Amministratore di sistema (ad interim): Michele Celeghini
- Gestione sviluppo prodotto: Michele Celeghini
- Design applicativo e analisi dati: Michele Gobbo

Misure che mirano a rischi e opportunità

Le aspettative delle parti interessate interne ed esterne sono descritte nel manuale del SG e nel documento Analisi del Contesto ed analisi dei Rischi in conformità ai requisiti della norma UNI CEI EN ISO/IEC 27001:2017 agg. al 20.06.2023.

L'organizzazione Azienda ha adottato e implementato la metodologia "Privacy Impact Analysis" (PIA) non solo per la gestione della privacy, ma estendendola a tutte le linee di sviluppo e servizio considerate critiche.

Obiettivi e traguardi, piani di realizzazione dell'IS

Gli obiettivi sono definiti a valle del riesame di direzione del 08.05.2023, tra cui:
1. certificazioni ISO 27001, entro ottobre 2023
2. adeguamento nuovi requisiti ACN, entro dicembre 2023

Risorse, competenze e consapevolezza

Mansionari e requisiti minimi di funzione non ancora formalizzati le responsabilità di sicurezza fondamentalmente in capo a 2 soli soggetti (1 interno ed 1 esterno).
Formazione tecnica per lo staff: Formazione su Emergenze es.
- attestato del corso di formazione per addetto alla prevenzione incendi, lotta antincendio e gestione delle emergenze, livello 1 4 ore, rilasciato il 23.03.2023 a T. M. Brambilla
- attestato del corso di formazione per addetto alla prevenzione incendi, lotta antincendio e gestione delle emergenze, rischio basso 4 ore, rilasciato il 23.03.2023 a T. M. Gobbo

Presente uno schema, non formalizzato, con tipologia di formazione per ruolo e storico formazione IT dal 2021.

Comunicazioni interne e informazioni documentate

La comunicazione interna è gestita in occasione di riunione di formazione e informazione, la comunicazione esterna avviene tramite telfono, sito web ed e-mail. Entrambi i processi sono supervisionati dalla direzione

2. DESCRIZIONE DEL SISTEMA E MATRICE DI CONFORMITA ISO/IEC 27001:2013

continuazione...

Pianificazione operativa e gestione

Politica sulla protezione dei dati personali valida dal 24.09.2020
Politica di Gruppo sul trattamento dei dati personali senza data revisione.
Codice etico rev. 2.0 del 29.11.2022
Regolamento interno Versione 1.7 del 09/02/2022

Procedure interne rev. 1.2 del 25.07.2022, include:
- gestione dei backup,
- change management applicativo e sistemistico,
- presidio e gestione continuità operativa e sicurezza,
- gestione incidenti di sicurezza,
- policy di sicurezza informatica
- gestione del personale
- gestione dei fornitori

Testbook compilati dall'utente ad ogni rilascio in produzione del software commissionato es.:
- 20221115_Testbook_MS1 _ EB_v.3_esiti per Testbook Task MS1 cliente Banca Euromobiliare, Collaudo del 07/11/2022, Produzione del 20/11/2022
- UAT wf crediti del 06 06 23.v1, Test Book cliente WF Crediti - Evolutive Maggio 2023 Collaudo del 05/06/2023 Produzione del 09/06/2023
- Report Analisi relativo al Progetto WF Crediti, ver. 1.9 del 05.04.2022

Valutazione del rischio e gestione / risoluzione dei rischi di informazione

Integrated Management System (IMS) Manual, rev. 1 del 20.06.2023, redatto secondo ISO 9001 and ISO 27001.

Valutazione del rischio all'interno del documento – Presidi di sicurezza logica alle infrastrutture AWS critiche ver. 1 del 01.06.2023.

Emessa la dichiarazione di applicabilità Versione 1.1 del 20 Giugno 2023, prevede l'applicabilità di tutti i punti dell'Annex A della ISO 27001 tranne:
- 8.3.3 Trasporto dei supporti fisici, poiché l'azienda non utilizza questa modalità
- 11.1.6 Aree di carico e scarico, poiché non sono presenti aree di carico e scarico nella struttura.

Il Piano di gestione del rischio all'interno del documento – Presidi di sicurezza logica alle infrastrutture AWS critiche ver. 1 del 01.06.2023, prevede le misure di valutazione dei rischi e il piano dei controlli
Es.:
CMT_Cloud del 07.12.2020
PIA_AssessmentWFC del 24.08.2020

Monitoraggio, misurazione, analisi, audit interni e riesami

Programma annuale audit interni 2023 emesso dalla direzione.

Registrazione dei risultati degli audit interni su SGSI, su documento Mod. 01.2_GAP Analysis_08.05.2023, nessuna NC rilevata.

Registro NC e AC senza registrazioni.

Riesame di direzione per SG integrato verbalizzato in data 08.05.2023 per il SG sicurezza delle informazioni.

Miglioramento

Miglioramenti pianificati tra gli elementi in uscita dal riesame di direzione del 08.05.2023, tra cui:
1. certificazioni ISO 27001, entro ottobre 2023
2. adeguamento nuovi requisiti ACN, entro dicembre 2023

Matrice di conformità - ISO/IEC 27001:2013

Elementi della norma	Livello di adempimento	Da verificare durante la sorveglianza successiva
Comprendere l'organizzazione e il suo contesto (4.1)		sì
Comprendere le necessità e le aspettative delle parti interessate (4.2)		sì
Determinare il campo di applicazione del SG per la sicurezza delle informazioni (4.3)		sì
Sistema di gestione per la sicurezza delle informazioni (4.4)		sì
Leadership (5)		sì
Azioni per affrontare rischi e opportunità (6.1)		sì
Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli (6.2)		sì
Risorse (7.1)		sì
Competenza (7.2)		sì
Consapevolezza (7.3)		sì
Comunicazione (7.4)		sì
Informazioni documentate (7.5)		sì
Pianificazione e controllo operativi (8.1)		sì
Valutazione del rischio per la sicurezza delle info. (8.2)		sì
Trattamento del rischio per la sicurezza delle info. (8.3)		sì
Monitoraggio, misurazione, analisi e valutazione (9.1)		sì
Audit interno (9.2)		sì
Riesame della direzione (9.3)		sì
Non conformità e azioni correttive (10.1)		sì
Miglioramento continuo (10.2)		sì

I requisiti standard sono soddisfatti ed i documenti di gestione risultano appropriati. Inadeguatezze notevoli sono riconosciute e rimosse durante il processo.

Requisiti standard e documenti di gestione sono appropriati. Le inadeguatezze non sono sempre riconosciute/rimosse o sono considerate come requisiti di trasparenza dello standard, senza benefici reali per l'azienda. L'auditor puo contemplare eccezioni.

I requisiti standard e i dossier di gestione posseduti non risultano appropriati. L'auditor opterà per una eccezione oppure per una non conformità, secondo l'entità e l'impatto sulla funzionalità del sistema.

A.5 Information security policies

Il documento di politica è all'interno del documento Politica e campo d'applicazione del 20.06.2023, include impegno al miglioramento continuo e al rispetto dei requisiti, alla soddisfazione dei clienti, alla prevenzione dell'inquinamento, degli infortuni e delle malattie professionali, alla prevenzione della corruzione, alla garanzia di sicurezza delle informazioni.
È comunicata internamente tramite affissione in bacheca e inviata alle parti interessate esterne che ne facciano richiesta

A.6 Organization of information security

Formazione e addestramento
Formazione tecnica per lo staff: Cartella "Formazione su Emergenze" file 2022_Formazione_Tecnici, es.
- attestato del corso di formazione per addetto alla prevenzione incendi, lotta antincendio e gestione delle emergenze, livello 1 4 ore, rilasciato il 23.03.2023 a T. M. Brambilla
- attestato del corso di formazione per addetto alla prevenzione incendi, lotta antincendio e gestione delle emergenze, rischio basso 4 ore, rilasciato il 23.03.2023 a T. M. Gobbo
-

Mansionari e requisiti minimi di funzione non ancora formalizzati REC, le responsabilità di sicurezza fondamentalmente in capo a 2 soli soggetti (1 interno ed 1 esterno).
Presente uno schema, non formalizzato, con tipologia di formazione per ruolo e storico formazione IT dal 2021.
La gestione dei sistemi mobili è gestita in accordo al documento "Regolamento per
il corretto utilizzo degli strumenti di lavoro" senza data di revisione.
Le politiche sono gestite centralmente dalla Federation applicata a livello di intero Gruppo Excellence mediante Microsoft 365 Business Premium ed applicate al medesimo modo agli endpoint di Excellence Innovation.
Si utilizza Microsoft Intune per consentire una gestione dei dati aziendali in sandbox e consentire il wipe automatico dei dati dall'amministratore in caso di necessità (smarrimento dispositivo, dimissioni) nonché il push di policy aggiuntive e di aggiornamenti.
Esempio attestazione presa in carico (servizio in outsourcing a capogruppo): Modulo Presa In Carico/Restituzione Dotazione Aziendale prot. 2023_PIC_RI_N°616_617 al sig. Marco Guidi del 25.01.2023, consegna di un laptop PCEXCC0131 Lenovo ThinkPad E14 Gen 2, S/N: PF-2BVN5B.
Applicate logiche di crittografia di Microsoft 365.

A.7 Human resource security

Recruiting Scheda di Valutazione, es. del 04.11.2022 senza registrazione di screening, solo di competenze.
Riferito che è in fase di studio interno un programma specifico di formazione SGSI per il personale, per il quale si è chiesto parere al DPO in data 26.05.2022.
Gestione utenze applicativo Gestite direttamente dai log di sistema (per la parte applicativa), mentre per la parte di gestione architetturale si usa il servizio AWS IAM (Identity Access Management) che consente la gestione granulare di ruoli e permessi.
Ultima cessazione di utenza a dominio: non utilizzato di recente.

A.8 Asset management

Visionato elenco risorse e dotazioni:
Elenco asset: Cartella "Policy Tecniche" file Mappatura-Istanze-Controlli(stralcio) agg. al 20.06.2023.
Excellence Innovation - Catalogo Dispositivi Endpoint utilizzati dall'azienda aggiornato al 20.06.2023, include 14 apparecchiature con dettaglio di Assegnatario, Marca, Modello e Sistema Operativo installato
Excellence Innovation - Catalogo Cespiti virtuali utilizzati per servizi SaaS, aggiornato al 20/06/2023, con dettaglio di Nome descrittivo dell'istanza, Tipologia Istanza AWS, Zona Geografica, Indirizzo interno Istanza AWS.

A.9 Access control

Politica sulla protezione dei dati personali valida dal 24.09.2020
Politica di Gruppo sul trattamento dei dati personali senza data revisione – REC
Codice etico rev. 2.0 del 29.11.2022
Regolamento interno Versione 1.7 del 09/02/2022
Procedure interne rev. 1.2 del 25.07.2022, include:
- gestione dei backup,
- change management applicativo e sistemistico,
- presidio e gestione continuità operativa e sicurezza,
- gestione incidenti di sicurezza,
- policy di sicurezza informatica
- gestione del personale
- gestione dei fornitori

A.10 Cryptography

Applicate logiche di crittografia di Microsoft 365.
Ogni cliente viene gestito separatamente dagli altri per quanto concerne l'architettura, che è comunque gestita da un unico account AWS.
- Infrastruttura informatica fisicamente gestita ed erogata da Amazon AWS su zona geografica Europea (Francoforte, Parigi, Irlanda), non condivisa logicamente con altri clienti (VPC dedicata);
- Componenti Server, Database e Storage separati e ridondati in standby nelle zone geografiche summenzionate. Le caratteristiche computazionali dell'istanza della componente server saranno definite in autonomia da Excellence in funzione dei volumi di utilizzo concordati, onde garantire fruizione adeguata da parte degli utenti sia all'avvio che durante l'erogazione a regime.
- Crittografia di alcuni dati sia su disco (con AES-256) ove la sensibilità dei dati lo richieda, sia in transito (con TLS 1.2) con chiavi dedicate;
- Monitoraggio automatico dell'uptime dell'infrastruttura e di eventuali issue di sicurezza con alerting per facilitare le eventuali operazioni di switchover manuale e segnalazione, attraverso sistemi AWS Cloudwatch, AWS Cloudtrail e AWS Guardduty.

A.11 Physical and environmental security

L'ufficio di sviluppo software, di una superficie complessiva di 250mq circa.
L'edificio è presidiato da una receptionist è presente durante le ore lavorative del mattino.
L'accesso all'ufficio è regolato attraverso:
- Citofono elettronico ad apertura manuale
- Sistema elettronico di controllo degli accessi "Sclak" alla porta principale dell'ufficio su cui ogni dipendente dispone di un'utenza nominativa.

Ogni ingresso e uscita viene registrato dal log del sistema, offrendo così un registro di tutte le persone che entrano ed escono dall'ufficio in qualsiasi momento. La concessione delle utenze nominative viene effettuata direttamente dal personale amministrativo e dirigente autorizzato mediante apposito pannello software.

A.12 Operations security

Politica sulla protezione dei dati personali valida dal 24.09.2020
Politica di Gruppo sul trattamento dei dati personali senza data revisione – REC
Codice etico rev. 2.0 del 29.11.2022
Regolamento interno Versione 1.7 del 09/02/2022
Procedure interne rev. 1.2 del 25.07.2022, include:
- gestione dei backup,
- change management applicativo e sistemistico,
- presidio e gestione continuità operativa e sicurezza,
- gestione incidenti di sicurezza,
- policy di sicurezza informatica
- gestione del personale
- gestione dei fornitori

Testbook compilati dall'utente ad ogni rilascio in produzione del software commissionato es.:
- 20221115_Testbook_MS1 _ EB_v.3_esiti per Testbook Task MS1 cliente Banca Euromobiliare, Collaudo del 07/11/2022, Produzione del 20/11/2022
- UAT wf crediti del 06 06 23.v1, Test Book cliente WF Crediti - Evolutive Maggio 2023 Collaudo del 05/06/2023 Produzione del 09/06/2023
- Report Analisi relativo al Progetto WF Crediti, ver. 1.9 del 05.04.2022

A.13 Communications security

Comunicazione interna gestita in occasione di riunione di formazione e informazione, comunicazione esterna gestita tramite mail e form di contatto dal sito web.

A.14 System acquisition, development and maintenance

Visionate:
- Mappatura-Istanze-Controlli per le logiche di inventariazione, monitoraggio, protezione ed accesso ad ognuna delle risorse tecniche
- Presidi di sicurezza logica alle infrastrutture AWS critiche report presidi tecnici del 01.06.2023

La verifica di cancellazione sicura dei dati residui sui dispositivi dismessi e di adeguatezza e compatibilità per la sicurezza delle informazioni da parte del resp. del sistema informatico; non si sono avuti casi di sviluppo di nuovi applicativi software; le nuove dotazioni hardware installate sono solo di tipo client e dotate di configurazione protetta nella intranet aziendale prima della messa a disposizione dell'utente.
Non presenti evidenze di dismissione di supporti di memorizzazione.

A.15 Supplier relationships

Politica sicurezza fornitori rev. 0 del 10.01.2022
Visionato accordo di riservatezza con amministratore sistema R. Cavalieri del 01.01.2020.

A.16 Information security incident management

Procedure interne rev. 1.2 del 25.07.2022, include:
- gestione dei backup,
- change management applicativo e sistemistico,
- presidio e gestione continuità operativa e sicurezza,
- gestione incidenti di sicurezza,
- policy di sicurezza informatica
- gestione del personale
- gestione dei fornitori

Incident report WFCREDI del 18/05/2022, simulazione di esaurimento dello spazio disponibile sul database server di produzione, combinato a mancato Alert sistemistico per un errore di configurazione della soglia di innesco dell'Alert stesso
Penetration Testing Report del 03.08.2022, con risultanze di una criticità di livello "low" e 2 "info", analizzate ed accettate.
Penetration Testing Report del 27.12.2022, con risultanze di una criticità di livello "low", analizzata e ancora aperta.
Password manager: One password gestito personalmente dal direttore generale M. Celeghini
Registro security vulnerability mensile da report AWS da Guarduty e Cloudwatch, agg. al 31.05.2023, aggiornato con frequenza mensile.
Report di controlli AWS di Amazon v. 1.4.0., 229 di 232 dei controlli superati; ultima sintesi mensile.
Vi è un elenco di eccezioni con alert silenziati in quanto valutati non necessari.
Registro monitoraggi security e performance da report AWS da Guarduty e Cloudwatch, agg. al 22.06.2023, aggiornato con frequenza bi-giornaliera.
Ultimo alert del 15.06.2023 da Cloudwatche, con seguito di chiarimenti sul canale Slack interno.

A.17 Information security aspects of business continuity management

Visionati:
- Piano di Business Continuity e Disaster Recovery ver. 1.0 del 13.06.2022
- procedura per la gestione di una violazione dei dati (Data Breach) valido dal 25.05.2018

che descrivono la gestione della continuità delle attività e dei processi in relazione ai rischi di: credito, reputazionale, operativo (endogeno, ossia rischio di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure aziendali, risorse umane inadeguate o sistemi operativi inefficaci; esogeno, derivante da perdite originate da eventi esterni), frodi interne ed esterne, personale e sicurezza sul lavoro, danni alle immobilizzazioni materiali, interruzione dell'attività e blocco dei sistemi informatici, errori operativi; valutati inoltre i rischi legati ai mutamenti dell'operatività aziendale (o rischio strategico); prevista la procedura di emergenza e di continuità operativa interna: sicurezza fisica, ridondanze, piano di recupero per guasto fisico e/o logico, schemi della infrastruttura virtualizzata.

continuazione...

A.18 Compliance

- Regolamento interno Versione 1.7 del 09/02/2022
- Procedure interne rev. 1.2 del 25.07.2022
- Registro dei trattamenti effettuati in qualità di responsabile
- Registro dei trattamenti del titolare e Lista Responsabili esterni

Lista dei documenti riesaminati - ISO/IEC 27001:2013

Nome del documento	No. del documento (o Data)	Riesaminato
Analisi del Contesto ed analisi dei Rischi	agg. al 20.06.2023	SÌ (CAAT)
Riesame di direzione	del 08.05.2023	SÌ (CAAT)
programma e report audit interni	del 08.05.2023	SÌ (CAAT)
Integrated Management System (IMS) Manual	rev. 1 del 20.06.2023	SÌ (CAAT)
organigramma	rev. 1 del 20.06.2023	SÌ (CAAT)
Dichiarazione di applicabilità	Versione 1.1 del 20 Giugno 2023	SÌ
Politica e campo d'applicazione	del 20.06.2023	SÌ
Politica sulla protezione dei dati personali	valida dal 24.09.2020	SÌ
Codice etico	rev. 2.0 del 29.11.2022	SÌ
Regolamento interno	Versione 1.7 del 09/02/2022	SÌ
Procedure interne	rev. 1.2 del 25.07.2022	SÌ
Presidi di sicurezza logica alle infrastrutture AWS critiche	ver. 1 del 01.06.2023	SÌ
dichiarazione di applicabilità	Versione 1.1 del 20 Giugno 2023	SÌ

SEDI VISITATE

Via Mauro Macchi, 32 20124 Milano (MI)
Central Function (HQ), Employees count: 9
Design and development

3. RIASSUNTO DEI RISULTATI DALLA VERIFICA

3.1. Punti di forza dell'organizzazione

ISO/IEC 27001:2013
Direzione presente e coinvolta; processi definiti e monitorati; rischi correttamente individuati e gestiti.

3.2. Non conformità e aree di miglioramento

Area di miglioramento 1
Si raccomanda di aggiornare l'inventory asset con tutti i dispositivi, le sedi, le infrastrutture e i ruoli aziendali.

ISO/IEC 27001:2013, Risorse (7.1)

Area di miglioramento 2
Procedere con le simulazioni di disaster recovery e business continuity.

ISO/IEC 27001:2013, Azioni per affrontare rischi e opportunità (6.1)

Area di miglioramento 3
Si raccomanda di apporre stato di revisione e data di aggiornamento su tutta la documentazione del sistema.

ISO/IEC 27001:2013, Informazioni documentate (7.5)

Area di miglioramento 4
Recuperare la documentazione relativa all'impianto anticendio (registro verifiche periodiche) e impianto elettrico (dichiarazione di conformità e verifiche periodiche di messa a terra).

ISO/IEC 27001:2013, Informazioni documentate (7.5)

Area di miglioramento 5
Formalizzare i mansionari e requisiti minimi di funzione.
Definire requisiti di screening pre-assuntivo per tutti i ruoli chiave e/o critici ai fini della sicurezza delle informazioni.

ISO/IEC 27001:2013, Competenza (7.2)

Riassunto delle non conformità e aree di miglioramento

Non conformità maggiore: 0
Non conformità minore: 0
Area di miglioramento: 5

3.5. Ostacoli incontrati che potrebbero compromettere l'attendibilità dei risultati e delle conclusioni dell'audit

Audit svolto regolarmente

4. AZIONI CONSEGUENTI, DISPOSIZIONI FINALI E RACCOMANDAZIONE

Grazie a tutti coloro che hanno partecipato all'organizzazione e anche a coloro che hanno partecipato alla verifica. Siamo lieti che l'audit del sistema di gestione nella vostra azienda funzioni adeguatamente e in un'atmosfera amichevole.

Risultati previsti
Il richiedente la certificazione (azienda certificata) è stato informato sull'idoneità della certificazione accreditata nel senso che: "per lo scopo definito di certificazione, un'organizzazione con un sistema di gestione certificato, che soddisfi e applica in modo appropriato i requisiti del sistema di gestione applicabile, può assicurare la fornitura permanente del suo servizio e / o dei suoi prodotti soddisfacendo le esigenze del cliente, le leggi e i regolamenti pertinenti al fine di aumentare la soddisfazione del cliente ".

Uso del Logo di LL-C
Dopo aver ottenuto un certificato valido il cliente ha diritto per la durata della validità del certificato all'uso di un logo approvato dall'ente di certificazione o di uno schema privato. In caso di certificazione del sistema, certificazione del processo o valutazione della completezza della documentazione tecnica, tale marchio non deve essere utilizzato su un prodotto o su una confezione di un prodotto visibile da possibili consumatori o/e in qualsiasi altro modo tale da indurre a un'interpretare il suddetto marchio come denotante la conformità di un prodotto specifico. L'uso e la collocazione del logo non devono creare confusione tra il cliente e la società di certificazione, né trasmettere una falsa impressione che la certificazione si applichi a un prodotto specifico anziché al sistema di gestione. Tali osservazioni hanno validità a meno che non si evinca chiaramente dallo schema di certificazione che non si fa riferimento alla valutazione di un prodotto specifico la cui conformità viene verificata in base a requisiti legali specificati in un documento normativo o legale.

Risoluzione delle non conformità e delle aree di miglioramento
I risultati dell'audit sono elencati nel capitolo precedente nella forma di Non conformità e Aree di miglioramento. Vi preghiamo cortesemente di regolarli come di seguito:

Non conformità maggiore
Se è stato trovata, deve essere formulata nel Protocollo di non conformità, che è allegato al presente rapporto. La non conformità maggiore è un tale inadempimento dei requisiti dello standard che il certificato non può essere rilasciato a meno che non ne sia terminata la risoluzione da parte del richiedente la certificazione. Quando una non conformità maggiore viene emessa durante un audit, il cliente deve fornire all'organismo di certificazione prove oggettive di un'indagine sui fattori causali e sui rischi che vengono esposti e sul loro piano d'azione correttivo proposto (PAC). Questo deve essere fornito entro 60 giorni dall'audit. La procedura di regolamento deve essere formulata dal richiedente sullo stesso modulo (Protocollo di non conformità). La non conformità maggiore deve essere chiusa entro ulteriori 30 giorni mediante l'attuazione di un'azione correttiva (CA) e la presentazione di prove all'OdC. Quando la non conformità è risolta l'audit può essere completato con risultati positivi. L'organismo di certificazione fornisce il metodo di verifica del regolamento di non conformità.

Non conformità minore
Una non-conformità minore è un inadempimento dei requisiti dello standard che permette il rilascio del certificato senza necessariamente terminare il regolamento della data NC minore da parte del richiedente. Un'analisi delle cause e un piano di azione correttivo proposto sono richiesti entro 30 giorni dall'audit. L'ente di certificazione deve essere informato dell'azione correttiva o dell'opposizione alla sua rilevanza entro 12 mesi dall'ultimo giorno dell'audit. L'azione correttiva relativa alla data NC minore è soggetta a controllo di sorveglianza o di ricertificazione. In caso di inadeguato assestamento la NC minore dovrebbe essere riclassificata come NC maggiore minacciando la validità del certificato.

Area di miglioramento
L'area di miglioramento è un commento mirato a migliorare il sistema di gestione o ad adempiere con maggiore efficienza determinati requisiti dello standard (si tratta principalmente della rimozione della conformità formale dei requisiti standard o dell'ottimizzazione delle soluzioni). in base ai criteri di accreditamento l'azienda certificata non è obbligata a rispondere attivamente a tali commenti, tuttavia molteplici aree di miglioramento ignorate possono risultare in una valutazione della performance del sistema negativa durante l'audit (o comunque ridotta rispetto al precedente audit).

Periodo di certificazione e validità del certificato
Il periodo, per il quale la società certificata si impegna a mantenere un sistema di gestione funzionale e l'organismo di certificazione è impegnato a fornire gli audit di sorveglianza corrisponde alla validità del certificato. Durante la sua validità, l'organismo di certificazione è obbligato a svolgere audit di sorveglianza ogni anno al posto delle attività aziendali certificate, a meno che un requisito normativo o legale non stabilisca eccezionalmente diversamente. Il primo audit di sorveglianza dopo la certificazione iniziale deve essere avviato entro 12 mesi dalla data di completamento dell'audit di certificazione; il secondo audit di sorveglianza deve essere avviato nel periodo annuale dalla data di completamento del primo audit di sorveglianza con una tolleranza massima di 45 giorni di calendario.

Prima della scadenza della validità del certificato verrà offerto un contratto con un possibile vantaggio sul prezzo per il successivo periodo di certificazione qualora il cliente sia interessato ad (lo scopo della certificazione rimarrà invariato). Per ottenere il vantaggio sul prezzo, l'audit / valutazione di ricertificazione deve essere effettuato prima della scadenza del certificato originale. Nei casi più gravi è possibile richiedere un rinvio della verifica di sorveglianza, tuttavia l'approvazione di questa esenzione è esclusivamente nelle mani dell'ente di certificazione. In caso di mancata collaborazione in un controllo di sorveglianza verrà intrapreso il processo di annullamento del certificato; tale procedura verrà resa pubblica secondo i criteri di accreditamento.

Obblighi del richiedente la certificazione
I principali obblighi dell'azienda certificata derivano dal contratto e dalle condizioni commerciali che ne sono parte.

Il titolare del certificato deve mantenere il proprio sistema di gestione funzionale per tutto il periodo di validità del certificato e applicare tutte le modifiche ai sistemi di gestione in base alle eventuali modifiche dei requisiti degli standard pertinenti o dei criteri di accreditamento basandosi sulle raccomandazioni inviate dall'ente di certificazione.

Inoltre, l'azienda certificata è obbligata a registrare e documentare tutti i reclami di terze parti relativi al proprio sistema di gestione e informare adeguatamente l'organismo di certificazione.

Obblighi dell'OdC / Organismo Notificato 2435

I doveri di base dell'ente di certificazione derivano dal contratto e dalle condizioni commerciali che ne fanno parte. L'organismo di certificazione è tenuto a mantenere il proprio stato di accreditamento, effettuare audit e sorveglianze regolarmente e secondo le date e gli intervalli di tempo specificati, e fornire obiettività nel determinare l'operabilità del sistema di gestione. Inoltre, l'organismo di certificazione è obbligato a monitorare le modifiche ai requisiti delle norme pertinenti e a notificare preventivamente tali cambiamenti alla società certificata, e elaborare i reclami e i dubbi sollevati dal cliente o da una terza parte in modo tempestivo.

Appello

Il richiedente della certificazione (società certificata) ha il diritto di presentare reclami contro la procedura dell'ente di certificazione o dei singoli revisori. Il reclamo del richiedente della certificazione (società certificata) deve essere inviato per iscritto. Allo stesso modo, il richiedente della certificazione (azienda certificata) può commentare questo rapporto. Un ricorso severo come un reclamo contro l'imparzialità dei revisori o contro la decisione dell'ente di certificazione di rifiutare l'emissione o il ritiro del certificato, è risolto dal Consiglio d'Appello indipendente entro 30 giorni. Altri commenti e obiezioni sono trattati a livello operativo in un appropriato periodo di tempo.

Rapporto di audit per terze parti

Questo rapporto riassume i risultati dell'audit. Il rapporto viene fornito al cliente in una copia in formato elettronico che viene inviata da LL-C (Certification). Il cliente ha il diritto di presentare a terzi esclusivamente il rapporto completo. Il contenuto di questo rapporto e tutti i record di controllo sono considerati confidenziali. Le segnalazioni possono essere presentate a terzi solo con il consenso del cliente o senza tale autorizzazione qualora l'ente di accreditamento e i proprietari di sistemi privati lo richiedano.

Raccomandazione

La 1a fase di audit è stata completata con successo. Il report di 1a fase è stato redatto e rilasciato all'organizzazione. Inoltre, il piano di audit e il team di audit sono stati confermati. Di conseguenza è iniziato la 2a fase di audit e ha riportato i seguenti risultati. L'obiettivo generale di audit (come specificato nel piano) è stato raggiunto. La conformità documentata del sistema di gestione è stata misurata attraverso processi altamente qualificati. Inoltre, l'attività del cliente è stata confrontata con i requisiti dello standard. È stato confermato che il sistema di gestione dell'organizzazione è in grado di soddisfare i requisiti applicabili degli standard pertinenti e ottenere i risultati attesi per la certificazione accreditata come indicato nel Comunicato ISO-IAF per la certificazione accreditata. L'organizzazione soddisfa e implementa appropriatamente i requisiti del sistema di gestione applicabili e può garantire la fornitura continua di questo servizio o prodotti in conformità ai requisiti del cliente e alle leggi e ai regolamenti vigenti al fine di aumentare la soddisfazione del cliente. Questa dichiarazione è stata fatta sulla valutazione del livello di adempimento dei requisiti del singolo standard, come evidenziato nella matrice di conformità di questo rapporto. Gli obiettivi dell'audit come specificato nella Sezione 1 - Ambito dell'Audit sono stati soddisfatti con successo. Inoltre, il campo di applicazione della certificazione è stato valutato come pienamente rappresentativo delle attività correnti dell'organizzazione.

In base all'esito dei risultati della verifica, si consiglia
di rilasciare il certificato di conformità del Sistema di Gestione ai requisiti dello standard **ISO/IEC 27001:2013**

per il campo di applicazione
Progettazione, sviluppo, installazione e assistenza di sistemi informativi e consulenze tecniche.

LL-C (Certification) Pietro Paolini

LL-C (Certification) Czech Republic a.s.
Pobřežní 620/3, 186 00 Praha 8 - Karlín
P. IVA 27118339