|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Dati relativi al triennio in oggetto** | | | | | | | | | | | | |
| Scopo | Scopo di certificazione | | | | | | | | | | | |
| Modifiche Scopo | NO  SI Anno/i: | | Norma / e (*Selezionare*): **ISO 27001** | | | | | | | | | |
| Triennio di riferimento | **201X – [gg.mm]** | | GG. uomo: **2** | | **201X - [gg.mm]** | | GG. uomo: **1** | | **201X - [gg.mm]** | | GG. uomo: **1** | |
| Gruppo Audit | LA | A | | Scegliere un elemento. | LA | A | | Scegliere un elemento. | LA | A | | Scegliere un elemento. |
| Nome Cognome | Nome Cognome | | Nome Cognome | Nome Cognome | Nome Cognome | | Nome Cognome | Nome Cognome | Nome Cognome | | Nome Cognome |
| Audit speciali | Tipo: | | | | Tipo: | | | | Tipo: | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Note Metodologiche** | | | |
| *Il presente check list si applica per la valutazione dei sistemi di gestione Integrati delle organizzazioni che erogano servizi o realizzano prodotti.*  *Esso è stato elaborato con riferimento ai requisiti delle norme ISO/IEC 27001 per i controlli previsti dall’ ANNEX A.*  *Il check list viene utilizzato come lista di controllo da parte dei valutatori nel corso delle visite di valutazione, di sorveglianza e di rinnovo svolte presso le organizzazioni che hanno attivato il processo di certificazione.*  *Il campo di applicazione, nonché i dettagli sulle eventuali esclusioni comprese delle relative giustificazioni devono essere resi disponibili in forma documentata.*  *È opportuno che i valutatori, durante le visite, prestino attenzione alla verifica del “campo di applicazione” e alle “esclusioni” dichiarate dall’organizzazione nella visita iniziale di Stage 1 sia a visita iniziale di Stage 2 (congruenza e conferma di quanto attestato nella Stage 1) che nelle successive visite di mantenimento o di rinnovo (conferma o aggiornamento del campo dell’SG certificato).* | | | |
| *Se indicata, la check-list integrativa deve essere consegnata unitamente alla presente e compilata in ogni sua parte. Per eventuali evidenze raccolte e registrate nella check-list integrativa è sufficiente far riferimento a quanto riportato nel suo pertinente punto (“v. requisito xx della check-list integrativa”)* | | | |
| **Legenda Acronimi** | **NC**: Non Conformità | **OSS**: Osservazione | **CM**: Commento |

|  |
| --- |
| **Argomenti da trattare nel corso del presente audit** |
| ***Riunione Iniziale****:*  *Presentazione del Gruppo di Audit di MY CERT e dei relativi compiti e responsabilità; Presentazione del personale dell’Organizzazione; Conferma degli impegni di riservatezza; Conferma della norma di valutazione; Conferma del numero di siti, impiegati, orario lavorativo (es. turnisti, part-time, chiusure per ferie ecc); Informazioni relative alle principali modifiche intervenute nell’organizzazione (personale, nuovi processi, attività, sedi/locali); Conferma dello scopo di certificazione (registrare lo scopo); Spiegazione di come si svolgerà la verifica, in particolare (Riferimento al piano di audit e ai canali di comunicazione durante l’audit, Conferma dell’esecuzione dell’audit in base a un campione delle informazioni disponibili, Descrizione dei rapporti di non conformità, Avviso tempestivo in caso di riscontro di non conformità, Necessità per gli auditor di intervistare altro personale oltre alla guida/e dell’Organizzazione, Conferma che l’Organizzazione sarà tenuta informata su come procede l’audit e di eventuali criticità, Riunione di chiusura e persone che devono presenziare); Conferma dello stato del sistema di gestione aziendale; Conferma della disponibilità delle guide; Conferma della disponibilità degli uffici/infrastrutture; Conferma degli accordi per la pausa pranzo; Conferma delle procedure relative alla salute e sicurezza, emergenze per il Gruppo di Audit; Invito a porre domande e/o chiedere chiarimenti; Disponibilità di tempo/collocazione per la riunione finale del Gruppo d’Audit.* |
| ***Riunione Finale****:*  *Ringraziamento all’Organizzazione per l’ospitalità, assistenza e collaborazione; Conferma della norma di riferimento utilizzata per l’audit; Conferma eventuali requisiti per schemi specifici; Conferma dello scopo di certificazione; Conferma dell’impegno alla riservatezza e del fatto che se qualche informazione reperita dovesse venire resa disponibile ad altri enti (ad es. all’organismo di accreditamento e/o altre autorità competenti), l’Organizzazione ne verrà informata; Informazione che le evidenze di audit raccolte sono basate su un campione delle informazioni disponibili; Spiegazione delle eventuali non conformità; Invito all’Organizzazione a discutere insieme le eventuali non conformità rilevate; Informazione all’Organizzazione sulla raccomandazione al rilascio/non rilascio del certificato o al suo mantenimento; Apposizione della firma dell’Organizzazione sul Rapporto d’Audit; Illustrazione delle procedure di reclamo e di ricorso (riferimento al sito web i MY CERT); Spiegazione e accordo sul processo relativo alle azioni correttive da intraprendere, incluse le scadenze per la loro presentazione (per l’audit iniziale e di rinnovo, l’evidenza delle azioni correttive deve essere presentata e verificata prima dell’emissione del certificato. Le evidenze devono essere presentate entro 15 giorni lavorativi); Spiegazione del processo di rilascio del certificato (solo per valutazione iniziale); Spiegazione organizzazione audit di sorveglianza; Conferma del possesso da parte del cliente di una copia del Regolamento nell’ultima revisione disponibile; Spiegazione del regolamento per l’utilizzo del marchio (solo per audit iniziale); Verifica dell’uso/non uso dei marchi (solo per audit di sorveglianza).* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rif. ISO /IEC 27001** | **Requisiti del Sistema di Gestione della Sicurezza delle Informazioni** | **Stato di implementazione** | **Commento** | **Evidenza** |
| **Rif** | **Requisito** |  |  |  |
| **4** | **Contesto dell’organizzazione** |  |  |  |
| 4.1 | L’organizzazione deve determinare i fattori esterni ed interni pertinenti alle sue finalità e che influenzano la sua capacità di conseguire gli esiti previsti per il proprio sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | Vedasi manuale del sistema di gestione integrato Ed. 01 rev. 00 del 02.02.2018 capitolo 4.1 L’ORGANIZZAZIONE E IL SUO CONTESTO |
| 4.2.a | L’organizzazione deve determinare le parti interessate pertinenti al sistema di gestione per la sicurezza delle informazioni | **applicato e formalizzato** |  | L'organizzazione ha detrminato le parti interessate: 4.2 COMPRENSIONE DELLE ESIGENZE E DELLE ASPETTATIVE DELLE PARTI INTERESSATE. 1. Clienti diretti 2. Legislatori, autorità competenti nazionali e europei, 3. Fornitori, 4. I Soci, 5. Istituti di credito, 6.Lavoratori |
| 4.2.b | L’organizzazione deve determinare i requisiti di tali parti interessate attinenti la sicurezza delle informazioni. | **applicato e formalizzato** |  | Determinati gli impatti in relazione specialmente alla privacy REG UE 679-2016 |
| 4.3 | L’organizzazione deve determinare i confini e l’applicabilità del sistema di gestione per la sicurezza delle informazioni per stabilirne il campo di applicazione. Il campo di applicazione deve essere disponibile come insieme di informazioni documentate. | **applicato e formalizzato** |  | Il campo di applicazione è stato definito |
| 4.3.a | Nel determinare il campo di applicazione, l’organizzazione deve considerare i fattori esterni ed interni di cui al punto 4.1 | **applicato e formalizzato** |  | Sono stati determinati i fattori interni ed esterni. Si riporta: • Risk management. L’azienda si è dotata di un piano di Business Continuity & Recovery Disaster. |
| 4.3.b | Nel determinare il campo di applicazione, l’organizzazione deve considerare i requisiti di cui al punto 4.2 | **applicato e formalizzato** |  | Considerati |
| 4.3.c | Nel determinare il campo di applicazione, l’organizzazione deve considerare le interfacce e le interdipendenze tra le attività svolte dall’organizzazione, e quelle svolte da altre organizzazioni | **applicato e formalizzato** |  | Considerati |
| 4.4 | L’organizzazione deve stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni, in conformità ai requisiti della presente norma internazionale. | **applicato e formalizzato** |  | L'azienda ha assegnato la leadership al rappresentante della direzione sig.re Massimo Pietra |
| **5** | **Leadership** |  |  |  |
| 5.1.a | L’alta direzione deve dimostrare leadership e impegno nei riguardi del sistema di gestione per la sicurezza delle informazioni: | **applicato e formalizzato** |  |  |
|  | a)        assicurando che la politica e gli obiettivi per la sicurezza delle informazioni siano stabiliti e siano compatibili con gli indirizzi strategici dell’organizzazione; | **applicato e formalizzato** |  | L'azienda ha definito la politca aziendale. Data politica: 02.02.2018 |
| 5.1 b | b)        assicurando l’integrazione dei requisiti del sistema di gestione per la sicurezza delle informazioni nei processi dell’organizzazione; | **applicato e formalizzato** |  | L'azienda ha definito la politca aziendale. Data politica: 02.02.2018 |
| 5.1.c | c)        assicurando la disponibilità delle risorse necessarie al sistema di gestione per la sicurezza delle informazioni; | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018 |
| **5.1.d** | **d)        comunicando l’importanza di un’efficace gestione della sicurezza delle informazioni e dell’essere conforme ai requisiti del sistema di gestione per la sicurezza delle informazioni;** | **applicato e formalizzato** |  | L'azienda ha impostato una campagna di comunicazione della politica attraverso la pubblicazione sul sito internet della stessa |
| 5.1.e | e)        assicurando che il sistema di gestione per la sicurezza delle informazioni consegua gli esiti previsti; | **applicato e formalizzato** |  | L'azienda ha definito li propri obiettivi in coerenza con le evidenze emerse dalla valutazione dei rischi |
| 5.1.f | f)         fornendo guida e sostegno alle persone per contribuire all’efficacia del sistema di gestione per la sicurezza delle informazioni; | **applicato e formalizzato** |  | L'azienda ha assegnato la leadership al rappresentante della direzione sig.re Massimo Pietra |
| 5.1.g | g)        promuovendo il miglioramento continuo; e | **applicato e formalizzato** |  | L'azienda ha assegnato la leadership al rappresentante della direzione sig.ra Massimo Pietra |
| 5.1.h | h)        fornendo sostegno ad altri pertinenti ruoli gestionali nel dimostrare la propria leadership come opportuno nelle rispettive aree di responsabilità. | **applicato e formalizzato** |  | L'azienda ha assegnato la leadership al rappresentante della direzione sig.ra Massimo Pietra |
| 5.2.a | L'alta direzione deve stabilire una politica per la sicurezza delle informazioni che: | **applicato e formalizzato** |  | L'azienda ha assegnato la leadership al rappresentante della direzione sig.ra Massimo Pietra |
|  | a)        sia appropriata alle finalità dell'organizzazione; | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018 |
| **5.2.b** | **b)        comprenda gli obiettivi per la sicurezza delle informazioni (vedere punto 6.2) o fornisca un quadro di riferimento per fissare gli obiettivi per la sicurezza delle informazioni;** | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018. Gli obiettivi sono enucleati nella politica |
| 5.2.c | c)        comprenda un impegno a soddisfare i requisiti applicabili e attinenti la sicurezza delle informazioni; e | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018. Gli impegni sono enucleati nella politica |
| 5.2.d | d)        comprenda un impegno per il miglioramento continuo del sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018. L'impegno al miglioramento continuo è enucleato nella politica |
| 5.2.e | La politica per la sicurezza delle informazioni deve: | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018 |
|  | e)        essere disponibile come insieme di informazioni documentate; | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018 |
| 5.2.f | f)         essere comunicata all'interno dell'organizzazione; | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018. Sul sito web |
| 5.2.g | g)        essere disponibile per le parti interessate, per quanto appropriato. | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018. Sul sito web |
| 5.3 | L’alta direzione deve assicurare che le responsabilità e le autorità per i ruoli pertinenti la sicurezza delle informazioni siano assegnati e comunicati. | **applicato e formalizzato** |  | L'azienda ha definito la politica aziendale. Data politica: 02.02.2018. L'azienda ha definito l'organigramma sia del SGSI che della privacy. |
| 5.3.a | L’alta direzione deve assegnare le responsabilità e autorità per: | **applicato e formalizzato** |  |  |
|  | **a)        assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti della presente norma internazionale; e** | **applicato e formalizzato** |  | L'azienda ha definito un SGSI in conformità ai punti della norma ISO 27001 |
| 5.3.b | b)        riferire all’alta direzione sulle prestazioni del sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | L'azienda ha definito un SGSI in conformità ai punti della norma ISO 27001 identificando un set di indicatori per tener sotto controllo le performance del SGSI |
| **6** | **Pianificazione** |  |  |  |
| 6.1.1.a | Nel pianificare il sistema di gestione per la sicurezza delle informazioni, l’organizzazione deve considerare i fattori di cui al punto 4.1 e i requisiti di cui al punto 4.2 e determinare i rischi e le opportunità che è necessario affrontare per: | **applicato e formalizzato** |  | L'azienda ha effettuato l'analisi dei rischi di tutti glia ssset aziendali che trattano informazioni. La valutazione dei rischi è stata effettuata in data 02.02.2018 e viene verificata ogni anno o qualora a fronte di attività di Ethical Hacking si evincano nuove vulnerabilità non previamente considerate |
|  | a)        assicurare che il sistema di gestione per la sicurezza delle informazioni possa conseguire gli esiti previsti; | **applicato e formalizzato** |  | Il sistema di gestione viene tenuto a livello prestazionale sotto controllo attraverso opportuni indicatori |
| 6.1.1.b | b)        prevenire, o ridurre, gli effetti indesiderati; e | **applicato e formalizzato** |  | Il sistema di gestione viene tenuto a livello prestazionale sotto controllo attraverso opportuni indicatori |
| 6.1.1.c | c)        realizzare il miglioramento continuo. | **applicato e formalizzato** |  | Il sistema di gestione viene tenuto a livello prestazionale sotto controllo attraverso opportuni indicatori |
| 6.1.1.d | L’organizzazione deve pianificare: | **applicato e formalizzato** |  |  |
|  | d)        le azioni per affrontare questi rischi e opportunità; e | **applicato e formalizzato** |  | L'azienda ha effettuato l'analisi dei rischi di tutti glia ssset aziendali che trattano informazioni. La valutazione dei rischi è stata effettuata in data 02.02.2018 e viene verificata ogni anno o qualora a fronte di attività di Ethical Hacking si evincano nuove vulnerabilità non previamente considerate |
| 6.1.1.e | e)        le modalità per | **applicato e formalizzato** |  |  |
|  | 1)        integrare e attuare le azioni nei processi del proprio sistema di gestione per la sicurezza delle informazioni; e | **applicato e formalizzato** |  | L'azienda ha effettuato l'analisi dei rischi di tutti glia ssset aziendali che trattano informazioni. La valutazione dei rischi è stata effettuata in data 02.02.2018 e viene verificata ogni anno o qualora a fronte di attività di Ethical Hacking si evincano nuove vulnerabilità non previamente considerate |
|  | 2)        valutare l’efficacia di tali azioni. | **applicato e formalizzato** |  | L'azienda ha effettuato l'analisi dei rischi di tutti glia ssset aziendali che trattano informazioni. La valutazione dei rischi è stata effettuata in data 02.02.2018 e viene verificata ogni anno o qualora a fronte di attività di Ethical Hacking si evincano nuove vulnerabilità non previamente considerate |
|  |  | **applicato e formalizzato** |  |  |
| 6.1.2.a | L’organizzazione deve definire e applicare un processo di valutazione del rischio relativo alla sicurezza delle informazioni che: | **applicato e formalizzato** |  |  |
|  | a)        stabilisca e mantenga i criteri di rischio relativo alla sicurezza delle informazioni, che includano: | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 1)        i criteri per l’accettazione del rischio; e | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 2)        i criteri per effettuare valutazioni del rischio relativo alla sicurezza delle informazioni; | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
| 6.1.2.b | b)        assicuri che ripetute valutazioni del rischio relativo alla sicurezza delle informazioni producano risultati coerenti, validi e confrontabili tra loro; | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
| 6.1.2.c | c)        identifichi i rischi relativi alla sicurezza delle informazioni: | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 1)        applicando il processo di valutazione del rischio relativo alla sicurezza delle informazioni per identificare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni; e | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 2)        identificando i responsabili dei rischi; | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
| 6.1.2.d | d)        analizzi i rischi relativi alla sicurezza delle informazioni: | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 1)        valutando le possibili conseguenze se i rischi identificati al punto 6.1.2 c) 1) si concretizzassero; | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 2)        valutando la verosimiglianza realistica del concretizzarsi dei rischi identificati al punto 6.1.2 c) 1); e | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 3)        determinando i livelli di rischio; | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
| 6.1.2.e | e)        ponderi i rischi relativi alla sicurezza delle informazioni: | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 1)        comparando i risultati dell’analisi del rischio con i criteri di rischio stabiliti al punto 6.1.2.a); e | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
|  | 2)        stabilendo le priorità dei rischi analizzati per il trattamento del rischio. | **applicato e formalizzato** |  | E' stata predisposta la procedura PR 6.1.1 Valutazione\_dei\_rischi\_e\_opportunita |
| 6.1.2 | L’organizzazione deve conservare informazioni documentate sul processo di valutazione del rischio relativo alla sicurezza delle informazioni. | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.1.3.a | L’organizzazione deve definire e applicare un processo di trattamento del rischio relativo alla sicurezza delle informazioni per: | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
|  | a)        selezionare le adeguate opzioni per il trattamento del rischio relativo alla sicurezza delle informazioni, tenendo in considerazione i risultati della valutazione del rischio; | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.1.3.b | b)        determinare tutti i controlli necessari per attuare le opzioni selezionate per il trattamento del rischio relativo alla sicurezza delle informazioni; | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.1.3.c | c)        confrontare i controlli determinati al punto 6.1.3.b) con quelli nell’Allegato A e verificare che non siano stati omessi controlli necessari; | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.1.3.d | d)        redigere una Dichiarazione di applicabilità che riporti i controlli necessari (vedere i punti 6.1.3 b) e c)) e le giustificazioni per l’inclusione, che siano attuati o meno, e per l’esclusione dei controlli dell’appendice A; | **applicato e formalizzato** |  | La dichiarazione di applicabilità è resa disponibile sul Modulo SGSI-01 |
| 6.1.3.e | e)        formulare un piano di trattamento del rischio relativo alla sicurezza delle informazioni; e | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.1.3.f | f)         ottenere l’approvazione del piano di trattamento del rischio relativo alla sicurezza delle informazioni e l’accettazione dei rischi residui relativi alla sicurezza delle informazioni da parte dei responsabili dei rischi. | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.1.3 | L’organizzazione deve conservare informazioni documentate sul processo di trattamento del rischio relativo alla sicurezza delle informazioni. | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
| 6.2 | L’organizzazione deve stabilire gli obiettivi per la sicurezza delle informazioni per le funzioni e per i livelli pertinenti. | **applicato e formalizzato** |  | La valutazione dei rischi è cristallizzata sul modulo 6.1.1.1 |
|  | Gli obiettivi per la sicurezza delle informazioni devono: | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | a)        essere coerenti con la politica per la sicurezza delle informazioni; | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | b)        essere misurabili (se possibile); | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | c)        tenere in considerazione i requisiti applicabili alla sicurezza delle informazioni e i risultati della valutazione del rischio e del trattamento del rischio; | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | d)        essere comunicati; e | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | e)        essere aggiornati per quanto appropriato. | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
| 6.2 | L’organizzazione deve conservare informazioni documentate sugli obiettivi per la sicurezza delle informazioni. | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
| 6.2 | Nel pianificare come conseguire i propri obiettivi per la sicurezza delle informazioni, l’organizzazione deve determinare: | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | a)        cosa sarà fatto; | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | b)        quali risorse saranno necessarie; | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | c)        chi ne sarà responsabile; | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | d)        quando sarà completato; e | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
|  | e)        come saranno valutati i risultati. | **applicato e formalizzato** |  | L'azienda ha definito un set di obiettivi |
| **7** | **Supporto** |  |  |  |
| 7.1 | L'organizzazione deve determinare e mettere a disposizione le risorse necessarie per stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | L'azienda ha definito l'organigramma del SGSI e il mansionario di ogni risorsa. I documenti riportano la data del 02.02.2018 |
| 7.2.a | L'organizzazione deve: | **applicato e formalizzato** |  |  |
|  | a)        determinare le necessarie competenze per le persone che svolgono attività sotto il suo controllo e che influenzano le sue prestazioni relative alla sicurezza delle informazioni; | **applicato e formalizzato** |  | L'azienda ha definito l'organigramma del SGSI e il mansionario di ogni risorsa. I documenti riportano la data del 02.02.2018 |
| 7.2.b | b)        assicurare che queste persone siano competenti sulla base di istruzione, formazione e addestramento o esperienza appropriate; | **applicato e formalizzato** |  | L'azienda ha definito il piano di formazione sul modulo di sistema M7.2.1.1 PROGRAMMA ATTIVITA' ADDESTRATIVA |
| 7.2.c | c)        ove applicabile, intraprendere azioni per acquisire la necessaria competenza e valutare l'efficacia delle azioni intraprese; e | **applicato e formalizzato** |  | L'azienda ha definito l'organigramma del SGSI e il mansionario di ogni risorsa. I documenti riportano la data del 02.02.2018 |
| 7.2.d | d)        conservare appropriate informazioni documentate quale evidenza delle competenze. | **applicato e formalizzato** |  | L'azienda ha definito l'organigramma del SGSI e il mansionario di ogni risorsa. I documenti riportano la data del 02.02.2018 |
| 7.3.a | Le persone che svolgono attività sotto il controllo dell’organizzazione devono essere consapevoli: | **applicato e formalizzato** |  | L'azienda ha definito una procedura operativa per la gestione di questo specifico aspetto: PR 7.2.1 GESTIONE DELLE RISORSE UMANE |
|  | a)        della politica per la sicurezza delle informazioni; | **applicato e formalizzato** |  | L'azienda ha definito una procedura operativa per la gestione di questo specifico aspetto: PR 7.2.1 GESTIONE DELLE RISORSE UMANE |
| 7.3.b | b)        del proprio contributo all’efficacia del sistema di gestione per la sicurezza delle informazioni, inclusi i benefici derivanti dal miglioramento delle prestazioni relative alla sicurezza delle informazioni; e | **applicato e formalizzato** |  | L'azienda ha definito una procedura operativa per la gestione di questo specifico aspetto: PR 7.2.1 GESTIONE DELLE RISORSE UMANE |
| 7.3.c | c)        delle implicazioni del non essere conformi ai requisiti del sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | L'azienda ha definito una procedura operativa per la gestione di questo specifico aspetto: PR 7.2.1 GESTIONE DELLE RISORSE UMANE |
| 7.4 | L’organizzazione deve determinare la necessità per le comunicazioni interne ed esterne in relazione al sistema di gestione per la sicurezza delle informazioni, includendo: | **applicato e formalizzato** |  | L'azienda come strumento di comunicazione utilizza il proprio sito web, e-mail ed informative allegate alle buste paga. |
|  | a) ciò su cui comunicare; | **applicato e formalizzato** |  |  |
|  | b) quando comunicare; | **applicato e formalizzato** |  |  |
|  | c) con chi comunicare; | **applicato e formalizzato** |  |  |
|  | d) chi deve comunicare; e | **applicato e formalizzato** |  |  |
|  | e) i processi attraverso i quali devono essere effettuate le comunicazioni. | **applicato e formalizzato** |  |  |
| 7.5.1 | Il sistema di gestione per la sicurezza delle informazioni dell’organizzazione deve comprendere: | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | a)        le informazioni documentate richieste dalla presente norma internazionale | **applicato e formalizzato** |  | Le procedure sono rispondenti alle informazioni documentate richieste |
|  | b)        le informazioni documentate che l'organizzazione ritiene necessarie per l'efficacia del sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | Le procedure sono rispondenti alle informazioni documentate richieste |
| 7.5.2 | Nel creare e aggiornare le informazioni documentate, l’organizzazione deve assicurare appropriati: | **applicato e formalizzato** |  | Le procedure sono rispondenti alle informazioni documentate richieste |
|  | a)        identificazione e descrizione (per esempio titolo, data, autore o numero di riferimento); | **applicato e formalizzato** |  | Le procedure sono rispondenti alle informazioni documentate richieste |
|  | b)        formato (per esempio lingua, versione del software, grafica) e supporto (per esempio cartaceo, elettronico); e | **applicato e formalizzato** |  | Le procedure sono rispondenti alle informazioni documentate richieste |
|  | c)        riesame e approvazione in merito all’idoneità e all’adeguatezza. | **applicato e formalizzato** |  | Le procedure sono rispondenti alle informazioni documentate richieste |
| 7.5.3 | Le informazioni documentate richieste dal sistema di gestione per la sicurezza delle informazioni e dalla presente norma internazionale devono essere tenute sotto controllo per assicurare che: | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | a)        siano disponibili e idonee all’uso, dove e quando necessario; e | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | b)        siano adeguatamente protette (per esempio da perdita di riservatezza, uso improprio o perdita d’integrità). | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | Il controllo delle informazioni documentate, da parte dell’organizzazione, deve riguardare le seguenti attività, per quanto applicabile: | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | c)        distribuzione, accesso, reperimento e uso; | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | d)        archiviazione e preservazione, compreso il mantenimento della leggibilità; | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | e)        tenuta sotto controllo delle modifiche (per esempio delle versioni); e | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | f)         conservazione e successive disposizioni. | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
|  | Le informazioni documentate di origine esterna ritenute necessarie dall'organizzazione per la pianificazione e per il funzionamento del sistema di gestione per la sicurezza delle informazioni, devono essere identificate per quanto appropriato, e tenute sotto controllo. | **applicato e formalizzato** |  | L'azienda ha predisposto la lista delle procedure operative attraverso il Modulo 7.5.1 |
| 8 | Attività operative | **applicato e formalizzato** |  |  |
| 8.1 | L’organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i requisiti di sicurezza delle informazioni e per mettere in atto le azioni determinate al punto 6.1. L’organizzazione deve anche attuare i piani per conseguire gli obiettivi per la sicurezza delle informazioni determinati al punto 6.2. | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
|  | L’organizzazione deve le conservare informazioni documentate nella misura necessaria ad avere fiducia che i processi siano stati eseguiti come pianificato. | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
|  | L’organizzazione deve tenere sotto controllo le modifiche pianificate e riesaminare le conseguenze dei cambiamenti involontari, intraprendendo azioni per mitigare qualunque effetto negativo, per quanto necessario. | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
|  | L’organizzazione deve assicurare che i processi affidati all’esterno siano determinati e tenuti sotto controllo. | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
| 8.2 | L’organizzazione deve effettuare le valutazioni del rischio relativo alla sicurezza delle informazioni a intervalli pianificati o quando sono proposti o si verificano cambiamenti significativi, considerando i criteri stabiliti al punto 6.1.2 a). | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
|  | L’organizzazione deve conservare informazioni documentate sui risultati delle valutazioni del rischio relativo alla sicurezza delle informazioni. | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
| 8.3 | L’organizzazione deve attuare il piano di trattamento del rischio relativo alla sicurezza delle informazioni. | **applicato e formalizzato** |  | Si veda la valutazione dei rischi per la sicurezza delle informazioni |
|  | L’organizzazione deve conservare informazioni documentate sui risultati del trattamento del rischio relativo alla sicurezza delle informazioni. | **applicato e formalizzato** |  | Vista la PR 6.1.3 Piano di trattamento del rischio |
| 9 | Valutazione delle prestazioni | **applicato e formalizzato** |  |  |
| 9.1 | L’organizzazione deve valutare le prestazioni della sicurezza delle informazioni e l’efficacia del sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | Visti gli obiettivi e indicatori efficacia controlli operativi aggiornata al 30.10.2018 |
|  | L’organizzazione deve determinare: | **applicato e formalizzato** |  |  |
|  | a)        cosa è necessario monitorare e misurare, includendo i processi e i controlli relativi alla sicurezza delle informazioni; | **applicato e formalizzato** |  |  |
|  | b)        i metodi per il monitoraggio, la misurazione, l’analisi e la valutazione, per quanto applicabile, per assicurare risultati validi; | **applicato e formalizzato** |  |  |
|  | c)        quando il monitoraggio e la misurazione devono essere effettuati; | **applicato e formalizzato** |  |  |
|  | d)        chi deve monitorare e misurare; | **applicato e formalizzato** |  |  |
|  | e)        quando i risultati del monitoraggio e della misurazione devono essere analizzati e valutati; e | **applicato e formalizzato** |  |  |
|  | f)         chi deve analizzare e valutare questi risultati. | **applicato e formalizzato** |  |  |
|  | L’organizzazione deve conservare appropriate informazioni documentate quale evidenza dei risultati dei monitoraggi e delle misurazioni. | **applicato e formalizzato** |  |  |
| 9.2 | L’organizzazione deve condurre, ad intervalli pianificati, audit interni per fornire informazioni tali da permettere di riconoscere se il sistema di gestione per la sicurezza delle informazioni: | **applicato e formalizzato** |  | L'azienda ha predisposto una procedura operativa PR 9.2 GESTIONE VERIFICHE ISPETTIVE |
|  | a)        è conforme ai | **applicato e formalizzato** |  |  |
|  | 1)        requisiti propri dell’organizzazione per il suo sistema di gestione per la sicurezza delle informazioni; e | **applicato e formalizzato** |  |  |
|  | 2)        requisiti della presente norma internazionale; | **applicato e formalizzato** |  |  |
|  | b)        è efficacemente attuato e mantenuto. | **applicato e formalizzato** |  |  |
|  | L’organizzazione deve: | **applicato e formalizzato** |  |  |
|  | c)        pianificare, stabilire, attuare e mantenere uno o più programmi di audit, comprensivi di frequenze, metodi, responsabilità, requisiti di pianificazione e reporting. I programmi di audit devono prendere in considerazione l’importanza dei processi coinvolti e i risultati di audit precedenti; | **applicato e formalizzato** |  |  |
|  | d)        definire i criteri di audit e il campo di applicazione per ciascun audit; | **applicato e formalizzato** |  |  |
|  | e)        selezionare gli auditor e condurre gli audit in modo da assicurare l’obiettività e l’imparzialità del processo di audit; | **applicato e formalizzato** |  |  |
|  | f)         assicurare che i risultati degli audit siano riportati ai pertinenti responsabili; e | **applicato e formalizzato** |  |  |
|  | g)        conservare informazioni documentate quale evidenza dell’attuazione del programma di audit e dei risultati di audit. | **applicato e formalizzato** |  |  |
| 9.3 | L’alta direzione deve, a intervalli pianificati, riesaminare il sistema di gestione per la sicurezza delle informazioni, per assicurarne la continua idoneità, adeguatezza ed efficacia. | **applicato e formalizzato** |  | Il riesame della direzione è programmato nella data del 29.11.2018 |
|  | Il riesame di direzione deve includere considerazioni su: | **applicato e formalizzato** |  |  |
|  | a)        lo stato delle azioni derivanti dai precedenti riesami di direzione; | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | b)        i cambiamenti dei fattori esterni e interni che hanno attinenza con il sistema di gestione per la sicurezza delle informazioni; | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | c)        le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni, compresi gli andamenti: | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | 1)        delle non conformità e azioni correttive; | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | 2)        dei risultati del monitoraggio e della misurazione; | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | 3)        dei risultati di audit; e | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | 4)        del raggiungimento degli obiettivi per la sicurezza delle informazioni; | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | d)        le informazioni di ritorno dalle parti interessate; | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | e)        i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio; e | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | f)         le opportunità per il miglioramento continuo. | **applicato e formalizzato** |  | Il riesame contepla il punto |
|  | Gli elementi in uscita dal riesame di direzione devono comprendere decisioni relative alle opportunità per il miglioramento continuo e ogni necessità di modifiche al sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | ok |
|  | L’organizzazione deve conservare informazioni documentate quale evidenza dei risultati dei riesami di direzione. | **applicato e formalizzato** |  | ok |
| 10 | Miglioramento | **applicato e formalizzato** |  | Gestito tramite la procedura PR 10.2\_AZIONI DI MIGLIORAMENTO |
| 10.1 | Quando si verifica una non conformità, l’organizzazione deve: | **applicato e formalizzato** |  |  |
|  | a)        reagire alla non conformità e, per quanto applicabile: | **applicato e formalizzato** |  |  |
|  | 1)        intraprendere azioni per tenerla sotto controllo e correggerla; e | **applicato e formalizzato** |  |  |
|  | 2)        fronteggiarne le conseguenze; | **applicato e formalizzato** |  |  |
|  | b)        valutare la necessità di azioni per eliminare le cause della non conformità, in modo che non si ripeta o non accada altrove: | **applicato e formalizzato** |  |  |
|  | 1)        riesaminando la non conformità; | **applicato e formalizzato** |  |  |
|  | 2)        determinando le cause della non conformità; e | **applicato e formalizzato** |  |  |
|  | 3)        determinando se esistono o potrebbero verificarsi non conformità simili; | **applicato e formalizzato** |  |  |
|  | c)        attuare ogni azione necessaria; | **applicato e formalizzato** |  |  |
|  | d)        riesaminare l’efficacia di ogni azione correttiva intrapresa; e | **applicato e formalizzato** |  |  |
|  | e)        effettuare, se necessario, modifiche al sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  |  |
|  | Le azioni correttive devono essere adeguate agli effetti delle non conformità riscontrate. | **applicato e formalizzato** |  |  |
|  | L’organizzazione deve tenere informazioni documentate quale evidenza: | **applicato e formalizzato** |  |  |
|  | f)         della natura delle non conformità e ogni successiva azione intrapresa, e | **applicato e formalizzato** |  |  |
|  | g)        dei risultati di ogni azione correttiva. | **applicato e formalizzato** |  |  |
|  |  | **applicato e formalizzato** |  |  |
| 10.2 | L’organizzazione deve migliorare in modo continuo l’idoneità, l’adeguatezza e l’efficacia del sistema di gestione per la sicurezza delle informazioni. | **applicato e formalizzato** |  | Si veda la procedura PR 10.1\_GESTIONE NC E AZIONI CORRETTIVE |

**CONTROLLI ANNEX A** – Data di applicazione: xx/xx/20XX

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.05.01 | **Indirizzi della direzione per la sicurezza delle informazioni** Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti. | | | |  |  |  |
| Controllo: | A.05.01.01 |  | **Politiche per la sicurezza delle informazioni** | | | |  |  |
|  | è stato definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti un insieme di politiche per la sicurezza delle informazioni? |  | Si veda la politica avente data 02.02.2018 | applicato e formalizzato |  |  |
| Controllo: | A.05.01.02 |  | **Riesame della politica per la sicurezza delle informazioni** | | | |  |  |
|  | Sono state riesaminate ad intervalli pianificati le politiche per la sicurezza delle informazioni o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l’idoneità, l’adeguatezza e l’efficacia? |  | Il riesame viene disciplinato dalla pr. 9.3 | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.06.01 | **Organizzazione interna** Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l’attuazione e l’esercizio della sicurezza delle informazioni all’interno dell’organizzazione. | | | |  |  |  |
| Controllo: | A.06.01.01 |  | **Ruoli e responsabilità per la sicurezza delle informazioni** | | |  |  |  |
|  | Sono state definite ed assegnate Tutte le responsabilità relative alla sicurezza delle informazioni? | Risulta nominato il DPO. | Si veda organigramma aziendale datato 02.02.2018 | applicato e formalizzato |  |  |
| Controllo: | A.06.01.02 |  | **Separazione dei compiti** | | |  |  |  |
|  | Sono state separati i compiti e le aree di responsabilità in conflitto tra loro per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell’organizzazione? |  | Si veda organigramma aziendale datato 02.02.2018 | applicato e formalizzato |  |  |
| Controllo: | A.06.01.03 |  | **Contatti con le autorità** | | |  |  |  |
|  | Sono mantenuti appropriati contatti con le autorità pertinenti? |  |  | non presente/non applicato |  |  |
| Controllo: | A.06.01.04 |  | **Contatti con gruppi specialistici** | | |  |  |  |
|  | Sono mantenuti appropriati contatti con gruppi specialistici o altri contesti ed associazioni professionali frequentate da specialisti della sicurezza delle informazioni? |  | Aziende specializzate in Ethical Hacking | applicato e formalizzato |  |  |
| Controllo: | A.06.01.05 |  | **Sicurezza delle informazioni nella gestione dei progetti** | | |  |  |  |
|  | La sicurezza delle informazioni è stata indirizzata nell’ambito della gestione dei progetti, a prescindere dal tipo di progetto? |  | Si veda la pr. 8.3 progettazione | applicato e formalizzato |  |  |
| Obiettivo: | A.06.02 | **Dispositivi portatili e telelavoro** Obiettivo: Assicurare la sicurezza del telelavoro e nell’uso di dispositivi portatili. | | | |  |  |  |
| Controllo: | A.06.02.01 |  | **Politica per i dispositivi portatili** | | |  |  |  |
|  | è stata adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall’uso di dispositivi portatili? | Vista la policy | SGSI-35 Procedura di sicurezza per laptop e dispositivi mobili | applicato e formalizzato |  |  |
| Controllo: | A.06.02.02 |  | **Telelavoro** | | |  |  |  |
|  | è stata attuata una politica e delle misure di sicurezza a suo supporto per proteggere le informazioni accedute, elaborate o memorizzate presso siti di telelavoro? | Non esistono telelavoratori | SGSI-42 Procedure di telelavoro e di lavoro mobile | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.07.01 | **Prima dell’impiego** Obiettivo: Assicurare che il personale e i collaboratori comprendano le proprie responsabilità e siano adatti a ricoprire i ruoli per i quali sono presi in considerazione. | | | |  |  |  |
| Controllo: | A.07.01.01 |  | **Screening** | | |  |  |  |
|  | Sono stati svolti dei controlli per la verifica del background effettuati su tutti i candidati all'impiego in accordo con le leggi, con i regolamenti pertinenti e con l'etica e sono gli stessi proporzionati alle esigenze di business, alla classificazione delle informazioni da accedere e ai rischi percepiti? |  | Si veda procedura PR 7.2.1\_GESTIONE DELLE RISORSE UMANE | applicato e formalizzato |  |  |
| Controllo: | A.07.01.02 |  | **Termini e condizioni di impiego** | | |  |  |  |
|  | Gli accordi contrattuali con il personale e con i collaboratori hanno specificato le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni? |  | Si veda procedura PR 7.2.1\_GESTIONE DELLE RISORSE UMANE | applicato e formalizzato |  |  |
| Obiettivo: | A.07.02 | **Durante l’impiego** Obiettivo: Assicurare che il personale e i collaboratori siano a conoscenza delle loro responsabilità per la sicurezza delle informazioni e vi adempiano. | | | |  |  |  |
| Controllo: | A.07.02.01 |  | **Responsabilità della direzione** | | |  |  |  |
|  |  |  | La direzione ha richiesto a tutto il personale e ai collaboratori di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione? |  | Si veda la politica aziendale ed il codice comportamentale approvato in ordine alla sicurezza delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.07.02.02 |  | **Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni** | | |  |  |  |
|  | Tutto il personale dell'organizzazione e, quando pertinente, i collaboratori, hanno ricevuto un’adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa? |  | Si veda la formazione erogata per il rispetto del reg. ue 679-2016 | applicato e formalizzato |  |  |
| Controllo: | A.07.02.03 |  | **Processo disciplinare** | | |  |  |  |
|  | è stato istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni? |  | Si veda la politica aziendale ed il codice comportamentale approvato in ordine alla sicurezza delle informazioni | applicato e formalizzato |  |  |
| Obiettivo: | A.07.03 | **Cessazione e variazione del rapporto di lavoro** Obiettivo: Tutelare gli interessi dell'organizzazione come parte del processo di variazione o di cessazione del rapporto di lavoro. | | | |  |  |  |
| Controllo: | A.07.03.01 |  | **Cessazione o variazione delle responsabilità durante il rapporto di lavoro** | | |  |  |  |
|  |  |  | Sono stati definiti, comunicati al personale o al collaboratore e resi effettivi le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro? |  | SGSI-04 Politica di gestione degli Asset | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.08.01 | **Responsabilità per gli asset** Obiettivo: Identificare gli asset dell’organizzazione e definire adeguate responsabilità per la loro protezione. | | | |  |  |  |
| Controllo: | A.08.01.01 |  | **Inventario degli asset** | | |  |  |  |
|  | Sono stati identificati tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni? è stato compilato e mantenuto aggiornato un inventario di questi asset? |  | SGSI-04 Politica di gestione degli Asset. SGSI-40 Procedura valutazione rischi | applicato e formalizzato |  |  |
| Controllo: | A.08.01.02 |  | **Responsabilità degli asset** | | |  |  |  |
|  |  |  | Gli asset censiti nell’inventario hanno un responsabile? |  | SGSI-04 Politica di gestione degli Asset. SGSI-40 Procedura valutazione rischi | applicato e formalizzato |  |  |
| Controllo: | A.08.01.03 |  | **Utilizzo accettabile degli asset** | | |  |  |  |
|  | Le regole per l’utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni sono state identificate, documentate e attuate? |  | SGSI-04 Politica di gestione degli Asset. SGSI-40 Procedura valutazione rischi | applicato e formalizzato |  |  |
| Controllo: | A.08.01.04 |  | **Restituzione degli asset** | | |  |  |  |
|  | Tutto il personale e gli utenti di parti esterne hanno restituito tutti gli asset dell’organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell’accordo stipulato? |  | SGSI-04 Politica di gestione degli Asset. SGSI-40 Procedura valutazione rischi. SGSI-27 Procedura Smaltimento di apparecchiature TIC | applicato e formalizzato |  |  |
| Obiettivo: | A.08.02 | **Classificazione delle informazioni** Obiettivo: Assicurare che le informazioni ricevano un adeguato livello di protezione in linea con la loro importanza per l’organizzazione. | | | |  |  |  |
| Controllo: | A.08.02.01 |  | **Classificazione delle informazioni** | | |  |  |  |
|  | Le informazioni sono state classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate? |  | SGSI-11 Politica di classificazione e trattamento delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.08.02.02 |  | **Etichettatura delle informazioni** | | |  |  |  |
|  |  |  | è stato sviluppato e attuato un appropriato insieme di procedure per l’etichettatura delle informazioni in base allo schema di classificazione adottato dall’organizzazione? |  | SGSI-11 Politica di classificazione e trattamento delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.08.02.03 |  | **Trattamento degli asset** | | |  |  |  |
|  |  |  | è stato sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall’organizzazione? |  | SGSI-11 Politica di classificazione e trattamento delle informazioni | applicato e formalizzato |  |  |
| Obiettivo: | A.08.03 | **Trattamento dei supporti** Obiettivo: Prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti. | | | |  |  |  |
| Controllo: | A.08.03.01 |  | **Gestione dei supporti rimovibili** | | |  |  |  |
|  | Sono state sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall’organizzazione? |  | SGSI-25 Procedura di gestione dei supporti di memorizzazione e protezione dei dati | applicato e formalizzato |  |  |
| Controllo: | A.08.03.02 |  | **Dismissione dei supporti** | | |  |  |  |
|  | La dismissione dei supporti non più necessari è avvenuta in modo sicuro, attraverso l’utilizzo di procedure formali? |  | SGSI-25 Procedura di gestione dei supporti di memorizzazione e protezione dei dati | applicato e formalizzato |  |  |
| Controllo: | A.08.03.03 |  | **Trasporto dei supporti fisici** | | |  |  |  |
|  | I supporti che contengono informazioni sono stati protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto? |  | SGSI-25 Procedura di gestione dei supporti di memorizzazione e protezione dei dati | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.09.01 | **Requisiti di business per il controllo degli accessi** Obiettivo: Limitare l’accesso alle informazioni ed ai servizi di elaborazione delle informazioni. | | | |  |  |  |
| Controllo: | A.09.01.01 |  | **Politica di controllo degli accessi** | | |  |  |  |
|  |  |  | è stata definita, documentata ed aggiornata una politica di controllo degli accessi sulla base dei requisiti di business e di sicurezza delle informazioni? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.01.02 |  | **Accesso alle reti e ai servizi di rete** | | |  |  |  |
|  |  |  | Sono stati forniti agli utenti solo degli accesi alle reti ed ai servizi di rete per il cui uso sono stati specificatamente autorizzati? |  | SGSI-24 Politica rete wireless | applicato e formalizzato |  |  |
| Obiettivo: | A.09.02 | **Gestione degli accessi degli utenti** Obiettivo : Assicurare l’accesso agli utenti autorizzati e prevenire accessi non autorizzati a sistemi e servizi. | | | |  |  |  |
| Controllo: | A.09.02.01 |  | **Registrazione e de-registrazione degli utenti** | | |  |  |  |
|  | è stato attuato un processo formale di registrazione e de-registrazione per abilitare l’assegnazione dei diritti di accesso? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.02.02 |  | **Provisioning degli accessi degli utenti** | | |  |  |  |
|  |  |  | è stato attuato un processo formale per l’assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.02.03 |  | **Gestione dei diritti di accesso privilegiato** | | |  |  |  |
|  |  |  | Sono stati limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.02.04 |  | **Gestione delle informazioni segrete di autenticazione degli utenti** | | |  |  |  |
|  | è stata controllata attraverso un processo di gestione formale l'assegnazione di informazioni segrete di autenticazione deve essere controllata? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.02.05 |  | **Riesame dei diritti di accesso degli utenti** | | |  |  |  |
|  | I responsabili degli asset hanno riesaminato ad intervalli regolari i diritti di accesso degli utenti? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.02.06 |  | **Rimozione o adattamento dei diritti di accesso** | | |  |  |  |
|  | I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni sono stati rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Obiettivo: | A.09.03 | **Responsabilità dell'utente** Obiettivo : Rendere gli utenti responsabili della salvaguardia delle loro informazioni di autenticazione. | | | |  |  |  |
| Controllo: | A.09.03.01 |  | **Utilizzo delle informazioni segrete di autenticazione** | | |  |  |  |
|  | Gli utenti devono essere tenuti a seguire le prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione. |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Obiettivo: | A.09.04 | **Controllo degli accessi ai sistemi e alle applicazioni** Obiettivo : Prevenire l'accesso non autorizzato a sistemi ed applicazioni. | | | |  |  |  |
| Controllo: | A.09.04.01 |  | **Limitazione dell’accesso alle informazioni** | | |  |  |  |
|  | L'accesso a informazioni e funzioni di sistemi applicativi è stato limitato secondo le politiche di controllo degli accessi? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.04.02 |  | **Procedure di log-on sicure** | | |  |  |  |
|  | è stato controllato da procedure di log-on sicure, quando richiesto dalle politiche di controllo degli accessi, l’accesso a sistemi e applicazioni? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.04.03 |  | **Sistema di gestione delle password** | | |  |  |  |
|  | I sistemi di gestione delle password sono interattivi e assicurano password di qualità? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.04.04 |  | **Uso di programmi di utilità privilegiati** | | |  |  |  |
|  | L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema è stato limitato e strettamente controllato? |  | SGSI-03 Politica di controllo degli accessi | applicato e formalizzato |  |  |
| Controllo: | A.09.04.05 |  | **Controllo degli accessi al codice sorgente dei programmi** | | |  |  |  |
|  | Gli accessi al codice sorgente dei programmi sono stati limitati? |  | SGSI-03 Politica di controllo degli accessi |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.10.01 | **Controlli crittografici** Obiettivo: Assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni. | | | |  |  |  |
| Controllo: | A.10.01.01 |  | **Politica sull’uso dei controlli crittografici** | | |  |  |  |
|  | è stata sviluppata e attuata una politica sull'uso dei controlli crittografici per la protezione delle informazioni? |  | SGSI-07 Politica di crittografia | applicato e formalizzato |  |  |
| Controllo: | A.10.01.02 |  | **Gestione delle chiavi** | | |  |  |  |
|  |  |  | è stata sviluppata e attuata una politica sull'uso, sulla protezione e sulla durata delle chiavi crittografiche attraverso il loro intero ciclo di vita? |  | SGSI-07 Politica di crittografia | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.11.01 | **Aree sicure** Obiettivo: Prevenire l’accesso fisico non autorizzato, danni e disturbi alle informazioni dell’organizzazione e alle strutture di elaborazione delle informazioni. | | | |  |  |  |
| Controllo: | A.11.01.01 |  | **Perimetro di sicurezza fisica** | | |  |  |  |
|  | Sono stati definiti ed usati dei perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.01.02 |  | **Controlli di accesso fisico** | | |  |  |  |
|  | Le aree di sicurezza sono protette da appropriati controlli per l’ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.01.03 |  | **Rendere sicuri uffici, locali e strutture** | | |  |  |  |
|  | è stata progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.01.04 |  | **Protezione contro minacce esterne ed ambientali** | | |  |  |  |
|  | è stata progettata e applicata un’adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.01.05 |  | **Lavoro in aree sicure** | | |  |  |  |
|  | Sono state progettate e attuate procedure per lavorare nelle aree sicure? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.01.06 |  | **Aree di carico e scarico** | | |  |  |  |
|  | I punti di accesso, come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, sono stati controllati e, se possibile, isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Obiettivo: | A.11.02 | **Apparecchiature** Obiettivo: Prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l’interruzione delle attività operative dell’organizzazione. | | | |  |  |  |
| Controllo: | A.11.02.01 |  | **Disposizione delle apparecchiature e loro protezione** | | |  |  |  |
|  | Le apparecchiature sono state disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.02.02 |  | **Infrastrutture di supporto** | | |  |  |  |
|  | Le apparecchiature sono state protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.02.03 |  | **Sicurezza dei cablaggi** | | |  |  |  |
|  | I cavi per l’energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi sono stati protetti da intercettazioni, interferenze o danneggiamenti? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.02.04 |  | **Manutenzione delle apparecchiature** | | |  |  |  |
|  |  |  | Le apparecchiature sono correttamente mantenute per assicurare la loro continua disponibilità e integrità? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.02.05 |  | **Trasferimento degli asset** | | |  |  |  |
|  |  |  | Apparecchiature, informazioni o software non sono stati portati all’esterno del sito senza preventiva autorizzazione? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.02.06 |  | **Sicurezza delle apparecchiature e degli asset all’esterno delle sedi** | | |  |  |  |
|  |  |  | Sono state previste misure di sicurezza per gli asset all’esterno delle sedi dell’organizzazione, considerando i diversi rischi derivanti dall’operare all’esterno dei locali dell’organizzazione stessa? |  | SGSI-38 Procedura per le infrastrutture fisiche e ambientali | applicato e formalizzato |  |  |
| Controllo: | A.11.02.07 |  | **Dismissione sicura o riutilizzo delle apparecchiature** | | |  |  |  |
|  |  |  | Tutte le apparecchiature contenenti supporti di memorizzazione sono state controllate per assicurare che ogni dato critico od il software concesso in licenza sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo? |  | SGSI-27 Procedura Smaltimento di apparecchiature TIC | applicato e formalizzato |  |  |
| Controllo: | A.11.02.08 |  | **Apparecchiature incustodite degli utenti** | | |  |  |  |
|  |  |  | Gli utenti hanno assicurato che le apparecchiature incustodite siano appropriatamente protette? |  | SGSI-18 Politica di protezione scrivania | applicato e formalizzato |  |  |
| Controllo: | A.11.02.09 |  | **Politica di schermo e scrivania puliti** | | |  |  |  |
|  |  |  | Sono state adottate sia una politica di “scrivania pulita” per i documenti ed i supporti di memorizzazione rimovibili, sia una politica di “schermo pulito” per i servizi di elaborazione delle informazioni? |  | SGSI-18 Politica di protezione scrivania | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.12.01 | **Procedure operative e responsabilità** Obiettivo: Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure. | | | |  |  |  |
| Controllo: | A.12.01.01 |  | **Procedure operative documentate** | | |  |  |  |
|  | Sono state documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano? |  | Sono state ideate 42 tra policy e procedure a supporto del SGSI | applicato e formalizzato |  |  |
| Controllo: | A.12.01.02 |  | **Gestione dei cambiamenti** | | |  |  |  |
|  | I cambiamenti all’organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni sono stati controllati? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |  |
| Controllo: | A.12.01.03 |  | **Gestione della capacità** | | |  |  |  |
|  | L’uso delle risorse è stato monitorato e messo a punto? Sono state fatte proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |  |
| Controllo: | A.12.01.04 |  | **Separazione degli ambienti di sviluppo, test e produzione** | | |  |  |  |
|  | Gli ambienti di sviluppo, test e produzione sono separati per ridurre il rischio di accesso o cambiamenti non autorizzati all’ambiente di produzione? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |  |
| Obiettivo: | A.12.02 | **Protezione dal malware** Obiettivo: Assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware. | | | |  |  |  |
| Controllo: | A.12.02.01 |  | **Controlli contro il malware** | | |  |  |  |
|  | Sono stati attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un’appropriata consapevolezza degli utenti? |  | SGSI-36 Procedura per software dannoso e antivirus | applicato e formalizzato |  |  |
| Obiettivo: | A.12.03 | **Backup** Obiettivo: Proteggere dalla perdita di dati. | | | |  |  |  |
| Controllo: | A.12.03.01 |  | **Backup delle informazioni** | | |  |  |  |
|  | Sono state effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata? |  | SGSI-10 Politica di backup e il ripristino delle informazioni | applicato e formalizzato |  |  |
| Obiettivo: | A.12.04 | **Raccolta di log e monitoraggio** Obiettivo: Registrare eventi e generare evidenze. | | | |  |  |  |
| Controllo: | A.12.04.01 |  | **Raccolta di log degli eventi** | | |  |  |  |
|  | La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni è stata effettuata, mantenuta e riesaminata periodicamente? |  | SGSI-10 Politica di backup e il ripristino delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.12.04.02 |  | **Protezione delle informazioni di log** | | |  |  |  |
|  | Le strutture per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati? |  | SGSI-10 Politica di backup e il ripristino delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.12.04.03 |  | **Log di amministratori e operatori** | | |  |  |  |
|  | Le attività degli amministratori e degli operatori di sistema sono sottoposte a log, e questi sono protetti e riesaminati periodicamente? |  | SGSI-10 Politica di backup e il ripristino delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.12.04.04 |  | **Sincronizzazione degli orolog** | | |  |  |  |
|  | Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all’interno di un’organizzazione o di un dominio di sicurezza sono sincronizzati rispetto a una singola sorgente temporale di riferimento? |  | SGSI-10 Politica di backup e il ripristino delle informazioni | applicato e formalizzato |  |  |
| Obiettivo: | A.12.05 | **Controllo del software di produzione** Obiettivo: Assicurare l’integrità dei sistemi di produzione. | | | |  |  |  |
| Controllo: | A.12.05.01 |  | **Installazione del software sui sistemi di produzione** | | |  |  |  |
|  | Sono state attuate procedure per controllare l’installazione del software sui sistemi di produzione? |  | SGSI-14 Politica di gestione operativa | applicato e formalizzato |  |  |
| Obiettivo: | A.12.06 | **Gestione delle vulnerabilità tecniche** Obiettivo: Prevenire lo sfruttamento di vulnerabilità tecniche. | | | |  |  |  |
| Controllo: | A.12.06.01 |  | **Gestione delle vulnerabilità tecniche** | | |  |  |  |
|  | Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati sono ottenute in modo tempestivo, l’esposizione a tali vulnerabilità è stata valutata e appropriate misure sono state intraprese per affrontare i rischi relativi? |  | SGSI-14 Politica di gestione operativa | applicato e formalizzato |  |  |
| Controllo: | A.12.06.02 |  | **Limitazioni all’installazione del software** | | |  |  |  |
|  | Sono state stabilite e attuate regole per il governo dell’installazione del software da parte degli utenti? |  | SGSI-14 Politica di gestione operativa | applicato e formalizzato |  |  |
| Obiettivo: | A.12.07 | **Considerazioni sull’audit dei sistemi informativi** Obiettivo: Minimizzare l’impatto delle attività di audit sui sistemi di produzione. | | | |  |  |  |
| Controllo: | A.12.07.01 |  | **Controlli per l’audit dei sistemi informativi** | | |  |  |  |
|  | I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione sono stati attentamente pianificati e concordati per minimizzare le interferenze con i processi di business? |  | SGSI-34 Procedura di audit interno | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.13.01 | **Gestione della sicurezza della rete** Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l’elaborazione delle informazioni a loro supporto. | | | |  |  |  |
| Controllo: | A.13.01.01 |  | **Controlli di rete** | | |  |  |  |
|  | Le reti devono sono gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni? |  | SGSI-24 Politica rete wireless | applicato e formalizzato |  |  |
| Controllo: | A.13.01.02 |  | **Sicurezza dei servizi di rete** | | |  |  |  |
|  | I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete sono stati identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall’interno o siano affidati all’esterno? |  | SGSI-24 Politica rete wireless | applicato e formalizzato |  |  |
| Controllo: | A.13.01.03 |  | **Segregazione nelle reti** | | |  |  |  |
|  | Nelle reti sono segregati gruppi di servizi, di utenti e di sistemi informativi? |  | SGSI-24 Politica rete wireless | applicato e formalizzato |  |  |
| Obiettivo: | A.13.02 | **Trasferimento delle informazioni** Obiettivo: Mantenere la sicurezza delle informazioni trasferite sia all’interno di un’organizzazione sia con qualsiasi entità esterna. | | | |  |  |  |
| Controllo: | A.13.02.01 |  | **Politiche e procedure per il trasferimento delle informazioni** | | |  |  |  |
|  | Esistono politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l’uso di tutte le tipologie di strutture di comunicazione? |  | SGSI-28 Procedura di controllo di documenti e registrazioni | applicato e formalizzato |  |  |
| Controllo: | A.13.02.02 |  | **Accordi per il trasferimento delle informazioni** | | |  |  |  |
|  | I trasferimenti sicuri di informazioni di business tra l’organizzazione e le parti esterne sono stati indirizzati in appositi accordi? |  | SGSI-28 Procedura di controllo di documenti e registrazioni | applicato e formalizzato |  |  |
| Controllo: | A.13.02.03 |  | **Messaggistica elettronica** | | |  |  |  |
|  | Le informazioni trasmesse attraverso messaggistica elettronica sono protette in modo appropriato? |  | SGSI-28 Procedura di controllo di documenti e registrazioni | applicato e formalizzato |  |  |
| Controllo: | A.13.02.04 |  | **Accordi di riservatezza o di non divulgazione** | | |  |  |  |
|  | I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell’organizzazione per la protezione delle informazioni sono stati identificati, riesaminati periodicamente e documentati? |  | SGSI-28 Procedura di controllo di documenti e registrazioni | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** |
| Obiettivo: | A.14.01 | **Requisiti di sicurezza dei sistemi informativi** Obiettivo: Assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi. Questo include anche i requisiti specifici per i sistemi informativi che forniscono servizi attraverso reti pubbliche. | | | |  |  |
| Controllo: | A.14.01.01 |  | **Analisi e specifica dei requisiti per la sicurezza delle informazioni** | | |  |  |
|  | I requisiti relativi alla sicurezza delle informazioni sono inclusi all’interno dei requisiti per i nuovi sistemi informativi o per l’aggiornamento di quelli esistenti? |  | SGSI-14 Politica di gestione operativa | applicato e formalizzato |  |
| Controllo: | A.14.01.02 |  | **Sicurezza dei servizi applicativi su reti pubbliche** | | |  |  |
|  | Le informazioni coinvolte nei servizi applicativi che transitano su reti pubbliche sono protette da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate? |  | SGSI-14 Politica di gestione operativa | applicato e formalizzato |  |
| Controllo: | A.14.01.03 |  | **Protezione delle transazioni dei servizi applicativi** | | |  |  |
|  | Le informazioni coinvolte nelle transazioni dei servizi applicativi sono protette al fine di prevenire trasmissioni incomplete, errori di instradamento, alterazione non autorizzata di messaggi, divulgazione non autorizzata, duplicazione non autorizzata di messaggi o attacchi di tipo "replay"? |  | SGSI-14 Politica di gestione operativa | applicato e formalizzato |  |
| Obiettivo: | A.14.02 | **Sicurezza nei processi di sviluppo e supporto** Obiettivo: Assicurare che la sicurezza delle informazioni sia progettata ed attuata all’interno del ciclo di sviluppo dei sistemi informativi. | | | |  |  |
| Controllo: | A.14.02.01 |  | **Politica per lo sviluppo sicuro** | | |  |  |
|  | Le regole per lo sviluppo del software e dei sistemi sono state stabilite ed applicate agli sviluppi all’interno dell’organizzazione? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.02 |  | **Procedure per il controllo dei cambiamenti di sistema** | | |  |  |
|  | I cambiamenti ai sistemi all’interno del ciclo di vita sono tenuti sotto controllo attraverso l’utilizzo di procedure formali di controllo dei cambiamenti? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.03 |  | **Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative** | | |  |  |
|  | Quando avvengono dei cambiamenti nelle piattaforme operative, le applicazioni critiche per il business sono state riesaminate e sottoposte a test per assicurare che non ci siano impatti negativi sulle attività operative dell’organizzazione o sulla sua sicurezza? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.04 |  | **Limitazioni ai cambiamenti dei pacchetti software** | | |  |  |
|  | La modifica dei pacchetti software è stata disincentivata e limitata ai cambiamenti necessari? Inoltre, tutti i cambiamenti sono strettamente controllati? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.05 |  | **Principi per l’ingegnerizzazione sicura dei sistemi** | | |  |  |
|  | I principi per l’ingegnerizzazione di sistemi sicuri sono stati stabiliti, documentati, manutenuti e applicati ad ogni iniziativa di implementazione di un sistema informativo? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.06 |  | **Ambiente di sviluppo sicuro** | | |  |  |
|  | Le organizzazioni hanno definito e protetto in modo appropriato ambienti di sviluppo sicuro per lo sviluppo dei sistemi e per le iniziative di integrazione che coprono l’intero ciclo di sviluppo dei sistemi? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.07 |  | **Sviluppo affidato all’esterno** | | |  |  |
|  | L’organizzazione ha supervisionato e monitorato l’attività di sviluppo dei sistemi affidata all’esterno? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.08 |  | **Test di sicurezza dei sistemi** | | |  |  |
|  | I test relativi alle funzionalità di sicurezza sono stati effettuati durante lo sviluppo? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Controllo: | A.14.02.09 |  | **Test di accettazione dei sistemi** | | |  |  |
|  | Sono stati stabiliti dei programmi di test e di accettazione ed i criteri ad essi relativi per i nuovi sistemi informativi, per gli aggiornamenti e per le nuove versioni? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |
| Obiettivo: | A.14.03 | **Dati di test** Obiettivo: Assicurare la protezione dei dati usati per il test. | | | |  |  |
| Controllo: | A.14.03.01 |  | **Protezione dei dati di test** | | |  |  |
|  | I dati di test sono stati scelti con attenzione, protetti e tenuti sotto controllo? |  | SGSI-33 Procedura di sviluppo e manutenzione dei sistemi informatici | applicato e formalizzato |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.15.01 | **Sicurezza delle informazioni nelle relazioni con i fornitori** Obiettivo: Assicurare la protezione degli asset dell’organizzazione accessibili da parte dei fornitori. | | | |  |  |  |
| Controllo: | A.15.01.01 |  | **Politica per la sicurezza delle informazioni nei rapporti con i fornitori** | | |  |  |  |
|  | I requisiti di sicurezza delle informazioni per mitigare i rischi associati all’accesso agli asset dell’organizzazione da parte dei fornitori sono stati concordati con i fornitori stessi e documentati? |  | SGSI-22 Politica di sicurezza per i fornitori | applicato e formalizzato |  |  |
| Controllo: | A.15.01.02 |  | **Indirizzare la sicurezza all’interno degli accordi con i fornitori** | | |  |  |  |
|  | Tutti i requisiti relativi alla sicurezza delle informazioni sono stati stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione? |  | SGSI-22 Politica di sicurezza per i fornitori | applicato e formalizzato |  |  |
| Controllo: | A.15.01.03 |  | **Filiera di fornitura per l’ICT (Information and Comunication Technology)** | | |  |  |  |
|  | Gli accordi con i fornitori includono i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l’ICT? |  | SGSI-22 Politica di sicurezza per i fornitori | applicato e formalizzato |  |  |
| Obiettivo: | A.15.02 | **Gestione dell’erogazione dei servizi dei fornitori** Obiettivo: Mantenere un livello concordato di sicurezza delle informazioni ed erogazione dei servizi in linea con gli accordi con i fornitori. | | | |  |  |  |
| Controllo: | A.15.02.01 |  | **Monitoraggio e riesame dei servizi dei fornitori** | | |  |  |  |
|  | Le organizzazioni provvedono regolarmente a monitorare, riesaminare e sottoporre a audit l’erogazione dei servizi da parte dei fornitori? |  | SGSI-22 Politica di sicurezza per i fornitori | applicato e formalizzato |  |  |
| Controllo: | A.15.02.02 |  | **Gestione dei cambiamenti ai servizi dei fornitori** | | |  |  |  |
|  | I cambiamenti alla fornitura dei servizi da parte dei fornitori, incluso il mantenimento e il miglioramento delle attuali politiche, procedure e controlli per la sicurezza delle informazioni, sono gestiti tenendo conto della criticità delle informazioni di business, dei sistemi e processi coinvolti e della rivalutazione dei rischi? |  | SGSI-22 Politica di sicurezza per i fornitori | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.16.01 | **Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti** Obiettivo: Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza. | | | |  |  |  |
| Controllo: | A.16.01.01 |  | **Responsabilità e procedure** | | |  |  |  |
|  | Sono state stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |
| Controllo: | A.16.01.02 |  | **Segnalazione degli eventi relativi alla sicurezza delle informazioni** | | |  |  |  |
|  | Gli eventi relativi alla sicurezza delle informazioni vengono segnalati il più velocemente possibile attraverso appropriati canali gestionali? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |
| Controllo: | A.16.01.03 |  | **Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni** | | |  |  |  |
|  | Viene richiesto a tutto il personale ed ai collaboratori che utilizzano i sistemi informativi ed i servizi dell’organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |
| Controllo: | A.16.01.04 |  | **Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni** | | |  |  |  |
|  | Gli eventi relativi alla sicurezza sono stati valutati ed è stato deciso se classificarli come incidenti relativi alla sicurezza delle informazioni? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |
| Controllo: | A.16.01.05 |  | **Risposta agli incidenti relativi alla sicurezza delle informazioni** | | |  |  |  |
|  | Si risponde agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |
| Controllo: | A.16.01.06 |  | **Apprendimento dagli incidenti relativi alla sicurezza delle informazioni** | | |  |  |  |
|  | La conoscenza acquisita dall’analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni viene utilizzata per ridurre la verosimiglianza o l’impatto degli incidenti futuri? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |
| Controllo: | A.16.01.07 |  | **Raccolta di evidenze** | | |  |  |  |
|  | L’organizzazione ha definito e applicato opportune procedure per l’identificazione, la raccolta, l’acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze? |  | SGSI-31 Procedura di segnalazione e gestione degli incidenti | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.17.01 | **Continuità della sicurezza delle informazioni** Obiettivo: La continuità della sicurezza delle informazioni deve essere integrata nei sistemi per la gestione della continuità operativa dell’organizzazione. | | | |  |  |  |
| Controllo: | A.17.01.01 |  | **Pianificazione della continuità della sicurezza delle informazioni** | | |  |  |  |
|  | L'organizzazione ha determinato i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri? |  | SGSI-29 Piano continuita operativa ITC | applicato e formalizzato |  |  |
| Controllo: | A.17.01.02 |  | **Attuazione della continuità della sicurezza delle informazioni** | | |  |  |  |
|  | L'organizzazione ha stabilito, documentato, attuato e mantenuto processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa? |  | SGSI-29 Piano continuita operativa ITC | applicato e formalizzato |  |  |
| Controllo: | A.17.01.03 |  | **Verifica, riesame e valutazione della continuità della sicurezza delle informazioni** | | |  |  |  |
|  | L'organizzazione verifica ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse? |  | SGSI-29 Piano continuita operativa ITC | applicato e formalizzato |  |  |
| Obiettivo: | A.17.02 | **Ridondanze** Obiettivo: Assicurare la disponibilità delle strutture per l’elaborazione delle informazioni. | | | |  |  |  |
| Controllo: | A.17.02.01 |  | **Disponibilità delle strutture per l’elaborazione delle informazioni** | | |  |  |  |
|  | Le strutture per l’elaborazione delle informazioni sono state realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità? |  | SGSI-29 Piano continuita operativa ITC | applicato e formalizzato |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Punto** | |  | **Descrizione** | **Commento** | **Evidenze** | **Applicato?** | **Spunti di miglioramento** | **Note** |
| Obiettivo: | A.18.01 | **Conformità ai requisiti cogenti e contrattuali** Obiettivo: Evitare violazioni a obblighi cogenti o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza. | | | |  |  |  |
| Controllo: | A.18.01.01 |  | **Identificazione della legislazione applicabile e dei requisiti contrattuali** | | |  |  |  |
|  | Per ogni sistema informativo e per l’organizzazione in generale sono stati esplicitamente definiti, documentati e mantenuti aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all’approccio stesso dell’organizzazione per soddisfarli? |  | Lista leggi applicabili | applicato e formalizzato |  |  |
| Controllo: | A.18.01.02 |  | **Diritti di proprietà intellettuale** | | |  |  |  |
|  | Sono state attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale potrebbero insistere diritti di proprietà intellettuale e per l'uso di prodotti software proprietari? |  | Non applicabile | applicato e formalizzato |  |  |
| Controllo: | A.18.01.03 |  | **Protezione delle registrazioni** | | |  |  |  |
|  | Le registrazioni sono protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business? |  | SGSI-11 Politica di classificazione e trattamento delle informazioni | applicato e formalizzato |  |  |
| Controllo: | A.18.01.04 |  | **Privacy e protezione dei dati personali** | | |  |  |  |
|  | Sono state assicurate la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile? | L'implementazione del GDPR deve essere completata | Manuale privacy del 25.05.2018. Mandati agli incaricati del trattamento. | applicato e formalizzato |  |  |
| Controllo: | A.18.01.05 |  | **Regolamentazione sui controlli crittografici** | | |  |  |  |
|  | I controlli crittografici sono utilizzati in conformità a tutti gli accordi, la legislazione e i regolamenti pertinenti? |  | SGSI-07 Politica di crittografia | applicato e formalizzato |  |  |
| Obiettivo: | A.18.02 | **Riesami della sicurezza delle informazioni** Obiettivo: Assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche e alle procedure dell’organizzazione. | | | |  |  |  |
| Controllo: | A.18.02.01 |  | **Riesame indipendente della sicurezza delle informazioni** | | |  |  |  |
|  | L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione (ossia, gli obiettivi di controllo, i controlli, le politiche, i processi e le procedure per la sicurezza delle informazioni) sono stati riesaminati in modo indipendente ad intervalli pianificati oppure quando si verificano cambiamenti significativi? |  | Si veda procedura PR 9.3\_Riesami del SGSI | applicato e formalizzato |  |  |
| Controllo: | A.18.02.02 |  | **Conformità alle politiche e alle norme per la sicurezza** | | |  |  |  |
|  | I responsabili hanno riesaminato regolarmente la conformità dei processi di elaborazione delle informazioni rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza? |  | Si veda procedura PR 9.3\_Riesami del SGSI | applicato e formalizzato |  |  |
| Controllo: | A.18.02.03 |  | **Verifica tecnica della conformità** | | |  |  |  |
|  | I sistemi informativi vengono regolarmente riesaminati per conformità con le politiche e con le norme per la sicurezza dell'organizzazione? |  | Si veda procedura PR 9.3\_Riesami del SGSI | applicato e formalizzato |  |  |