|  |  |  |  |
| --- | --- | --- | --- |
| **req** | ISO 27001 **REQUISITI** | | **EVIDENZE E DOCUMENTI DA FORNIRE** |
| 5.1 | Policies for information security | La politica di sicurezza delle informazioni e le politiche specifiche per argomento devono essere definite, approvate dalla direzione, pubblicate, comunicate e riconosciute dal personale competente e dalle parti interessate rilevanti e riesaminate a intervalli pianificati e se si verificano cambiamenti significativi. | * Politica generale di sicurezza delle informazioni * Elenco dei documenti ISMS * Analisi del contesto e delle parti interessate * SOA (Dichiarazione di applicabilità dei controlli) * Analisi dei rischi di sicurezza delle informazioni * Organigramma * Mansionario |
| 5.2 | Information security roles and responsibilities | I ruoli e le responsabilità in materia di sicurezza delle informazioni devono essere definiti e assegnati in base alle esigenze dell'organizzazione. | Organigramma |
| 5.3 | Segregation of duties | I doveri conflittuali e le aree di responsabilità conflittuali sono separati. | Documentazione o Politica o procedura sulla segregazione dei compiti (Da predisporre) |
| 5.4 | Management responsibilities | La direzione deve richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con la politica di sicurezza delle informazioni stabilita, le politiche e le procedure specifiche dell'organizzazione. | Evidenza di richiesta ai dipendenti della direzione all’applicazione della politica e dei controlli.   * Copie delle clausole contrattuali * Nomine incaricati al trattamento dati * NDA * Nomina DPO * Nomina Amministratore di sistema |
| 5.5 | Contact with authorities | L'organizzazione deve stabilire e mantenere contatti con le autorità competenti. | Nell’organigramma e/o nel mansionario e/o in altro documento, verificare chi deve avere contati con le autorità (Garante Privacy, GdF, Enti di certificazione, Polizia Postale)   * Nomina di chi è autorizzato alle comunicazioni con le autorità * Nomina del DPO |
| 5.6 | Contact with special interest groups | L'organizzazione deve stabilire e mantenere contatti con gruppi di interesse speciali o altri forum specializzati in materia di sicurezza e associazioni professionali. | Evidenza di iscrizione Privacy: Contatti/contratti con I consulenti GDPR   * IT-Security: Contatti/Contratti con il fornitore IT * IT-Security: Contratti/contratti con SOC esterna * IT-Security: elencare forum e bollettini seguiti n tema di sicurezza IT |
| 5.7 | Threat intelligence | Le informazioni relative alle minacce alla sicurezza delle informazioni sono raccolte e analizzate per produrre informazioni sulle minacce. | È necessario che sia predisposta una procedura che prenda in considerazione almeno le seguenti fasi:   * strutturare una metodologia per raccogliere informazioni sulle minacce (vedi 5.6) * analizzare le minacce per il contesto di riferimento * diffondere le informazioni sulle minacce all’interno dell’Organizzazione * analizzare l’efficacia della diffusione * verificare che vi sia un piano formativo sulle principali minacce   Screen shot dei risultati dei tool utilizzati per la Threat Intelligence |
| 5.8 | Information security in project management | La sicurezza delle informazioni è integrata nella gestione dei progetti. | Verificare che sia presente documentazione per:   * definire i requisiti di sicurezza delle informazioni per il progetto, comprese le esigenze aziendali e gli obblighi legali. * Valutare gli impatti dei rischi derivanti dalle minacce alla sicurezza delle informazioni. * Gestire gli impatti del rischio implementando controlli e processi appropriati. * Monitorare e riferire sull'efficacia di tali controlli.   Per proteggere i progetti aziendali, l’ente deve assicurarsi che tutti i project manager siano consapevoli della sicurezza delle informazioni e la seguano mentre completano il loro lavoro.  Tali informazioni possono trovarsi su un project charter o su una meeting minute o su un kick off report.  Verificare che l’organizzazione, nell’ambito dei contratti (progetti) che ha con i propri clienti, stabilisce, con il cliente, una serie di misure di sicurezza. |
| 5.9 | Inventory of information and other associated assets | È elaborato e mantenuto un inventario delle informazioni e degli altri beni associati, compresi gli owner. | * Inventario delle informazioni da proteggere, ciascuna correlata ai beni strumentali su cui sono queste informazioni. * File Excel Asset Inventory. |
| 5.10 | Acceptable use of information and other associated assets | Le norme per l'uso accettabile e le procedure per il trattamento delle informazioni e di altri beni associati sono individuate, documentate e attuate. | * Procedure e norme per l’uso accettabile degli strumenti informatici e delle informazioni in essi contenuti * Registrazioni di assegnazione degli asset |
| 5.11 | Return of assets | Il personale e le altre parti interessate, a seconda dei casi, restituiscono tutti i beni dell'organizzazione in loro possesso in caso di modifica o cessazione del loro rapporto di lavoro, contratto o accordo. | * Procedura di riconsegna degli asset al cambio mansione e/o alla cessazione del lavoro * Registrazioni di riconsegna degli asset |
| 5.12 | Classification of information | Le informazioni sono classificate in base alle esigenze di sicurezza dell'organizzazione in base alla riservatezza, all'integrità, alla disponibilità e ai requisiti pertinenti delle parti interessate. | Le informazioni devono essere classificate su una scala di accesso (pubblico, ristretto, confidenziale, strettamente confidenziale). Le informazioni devono essere classificate in base alle proprie caratteristiche SRID.  Verificare procedura/politica di classificazione delle informazioni. |
| 5.13 | Labelling of information | Deve essere sviluppata e attuata un'adeguata serie di procedure per l'etichettatura delle informazioni conformemente allo schema di classificazione delle informazioni adottato dall'organizzazione. | Stabilire una politica di etichettatura delle informazioni tipo:   * pubblico * ristretto * confidenziale * strettamente confidenziale * collegata ai rischi ad esse collegate.   Come sopra |
| 5.14 | Information transfer | Le regole, le procedure o gli accordi sul trasferimento delle informazioni devono essere in vigore per tutti i tipi di strutture di trasferimento all'interno dell'organizzazione e tra l'organizzazione e le altre parti. | Procedura/politica sulle misure di sicurezza per il trasferimento/invio delle informazioni. |
| 5.15 | Access control | Le norme per controllare l'accesso fisico e logico alle informazioni e ad altri beni associati sono stabilite e attuate sulla base dei requisiti di sicurezza delle imprese e delle informazioni. | Procedura/politica di accesso logico alle informazioni.  Procedura/politica di accesso fisico alle informazioni.  Screen shot di schermate di login |
| 5.16 | Identity management | È gestito l'intero ciclo di vita delle identità. | Procedura/politica atta a consentire l'identificazione univoca di individui e sistemi che accedono alle informazioni dell'organizzazione e ad altre risorse associate e consentire un'assegnazione appropriata e una pronta revoca dei diritti di accesso. |
| 5.17 | Authentication information | L'assegnazione e la gestione delle informazioni di autenticazione sono controllate da un processo di gestione, compresa la consulenza al personale in merito al trattamento appropriato delle informazioni di autenticazione. | Come sopra  Screen shot di schermate (es. e-mail) di assegnazione/de-assegnazione di profili |
| 5.18 | Access rights | I diritti di accesso alle informazioni e ad altre risorse associate devono essere forniti, rivisti, modificati e rimossi in conformità con la politica tematica e le regole per il controllo dell'accesso dell'organizzazione. | Come sopra  Fornire documento esempio. |
| 5.19 | Information security in supplier relationships | I processi e le procedure devono essere definiti e implementati per gestire i rischi per la sicurezza delle informazioni associati all'uso dei prodotti o dei servizi del fornitore. | Verificare che l’organizzazione reperisca la documentazione di sicurezza e privacy dei sistemi dei fornitori. |
| 5.20 | Addressing information security within supplier agreements | I pertinenti requisiti di sicurezza delle informazioni sono stabiliti e concordati con ciascun fornitore in base al tipo di rapporto con lo stesso. | Specifica dei requisiti di sicurezza sui contratti e, in generale, presenza di documentazione dei requisiti di sicurezza del rapporto con i fornitori.  Evidenze: Clausole contrattuali di sicurezza delle informazioni e privacy con i fornitori. |
| 5.21 | Managing information security in the information and communication technology (ICT) supply chain | Sono definiti e attuati processi e procedure per gestire i rischi per la sicurezza delle informazioni associati alla catena di fornitura di prodotti e servizi ITC. | * Implementare una politica specifica * Implementare un processo di gestione dei fornitori * Includere nel processo di gestione dei fornitori l'acquisizione e il trasferimento degli stessi * Implementare un registro dei fornitori di terze parti * Avere accordi con tutti i fornitori che incidono sui requisiti di sicurezza delle informazioni * Avere garanzie di sicurezza delle informazioni per i fornitori critici (come minimo e idealmente per tutti i fornitori rilevanti) |
| 5.22 | Monitoring, review and change management of supplier Services | L'organizzazione deve monitorare, rivedere, valutare e gestire regolarmente i cambiamenti nelle pratiche di sicurezza delle informazioni dei fornitori e nell'erogazione del Servizio. | Piani dei controlli di revisione delle politiche e degli accordi con i fornitori e dei loro requisiti di sicurezza. |
| 5.23 | Information security for use of cloud Services. | I processi per l'acquisizione, l'utilizzo, la gestione e l'uscita dai Servizi cloud devono essere stabiliti in conformità con i requisiti di sicurezza delle informazioni dell'organizzazione. | Va notato che ISO considera l'aderenza a Control 5.23 come uno sforzo collaborativo tra l'organizzazione e il proprio partner di servizi cloud.  Il controllo 5.23 dovrebbe inoltre essere strettamente allineato con i controlli 5.21 e 5.22, che riguardano rispettivamente la gestione delle informazioni nella catena di approvvigionamento e la gestione dei servizi ai fornitori.  L'organizzazione dovrebbe definire:   1. qualsiasi requisito di sicurezza pertinente o preoccupazione relativa all'uso di una piattaforma cloud; 2. i criteri coinvolti nella selezione di un provider di servizi cloud e come devono essere utilizzati i relativi servizi; 3. in modo granulare i ruoli e le responsabilità rilevanti che regolano il modo in cui i servizi cloud devono essere utilizzati in tutta l'organizzazione; 4. esattamente quali aree di sicurezza delle informazioni sono controllate dal fornitore di servizi cloud e quelle che rientrano nelle competenze dell'organizzazione stessa; 5. i modi migliori in cui prima raccogliere e poi utilizzare tutti i componenti del servizio relativi alla sicurezza delle informazioni forniti dalla piattaforma di servizi cloud; 6. come ottenere garanzie categoriche su eventuali controlli relativi alla sicurezza delle informazioni attuati dal provider di servizi cloud; 7. i passaggi che devono essere intrapresi per gestire le modifiche, le comunicazioni e i controlli su più piattaforme cloud distinte e non sempre dallo stesso fornitore; 8. procedure di Incident Management che riguardano esclusivamente l'erogazione dei servizi cloud; 9. come l'organizzazione prevede di gestire l'uso continuo e/o l'adozione all'ingrosso delle piattaforme cloud, in linea con i più ampi obblighi di sicurezza delle informazioni; 10. una strategia per la cessazione o la modifica dei servizi cloud, sia su base fornitore per fornitore, sia attraverso il processo di migrazione da cloud a on-premise.   Evidenze: Documentazione di sicurezza dei SAAS approvvigionati (generalmente reperibili via internet. Tutti i fornitori di SAAS pubblicano le politiche, i documenti privacy compliance, le certificazioni di sicurezza IT, un abstract sui risultati dei VA/PT) |
| 5.24 | Information security incident management planning and preparation. | L'organizzazione deve pianificare e prepararsi alla gestione degli incidenti di sicurezza delle informazioni definendo, stabilendo e comunicando processi, ruoli e responsabilità di gestione degli incidenti di sicurezza delle informazioni. | * Procedura / politica sulla gestione degli incidenti di sicurezza delle informazioni * Evidenze di rilevamento e gestione degli incidenti * Evidenze di soluzioni contro gli eventi che hanno causato tali incidenti |
| 5.25 | Assessment and decision on information security events | L'organizzazione deve valutare gli eventi di sicurezza delle informazioni e decidere se devono essere classificati come incidenti di sicurezza delle informazioni. |
| 5.26 | Response to information security incidents | Gli incidenti di sicurezza delle informazioni devono essere risolti conformemente alle procedure documentate. |
| 5.27 | Learning from information security incidents | Le conoscenze acquisite dagli incidenti di sicurezza delle informazioni sono utilizzate per rafforzare e migliorare i controlli di sicurezza delle informazioni. |
| 5.28 | Collection of evidence | L'organizzazione deve stabilire e attuare procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove relative agli eventi di sicurezza delle informazioni. |
| 5.29 | Information security during disruption | L'organizzazione deve decidere come mantenere la sicurezza delle informazioni ad un livello adeguato durante le interruzioni. |
| 5.30 | ICT readiness for business continuity | La prontezza alle ITC è pianificata, attuata, mantenuta e testata sulla base degli obiettivi di continuità operativa e dei requisiti di continuità delle ICT. | * Procedura e/o politica relativa alla continuità operativa * Registrazioni di test eseguiti per verificare la procedura/politica di continuità operativa |
| 5.31 | Legal, statutory, regulatory and contractual requirements | I requisiti legislativi, normativi, normativi e contrattuali relativi alla sicurezza delle informazioni e l'approccio dell'organizzazione per soddisfare tali requisiti devono essere identificati, documentati e aggiornati. | Fornire esempi di clausole contrattuali con clienti riguardanti la sicurezza delle informazioni |
| 5.32 | Intellectual property rights | L'organizzazione attua procedure appropriate per proteggere i diritti di proprietà intellettuale. | N/A. |
| 5.33 | Protection of records | Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato. | A valle della valutazione dei rischi |
| 5.34 | Privacy and protection of person-al identifiable information (PII) | L'organizzazione deve identificare e soddisfare i requisiti relativi alla tutela della privacy e alla protezione delle PII secondo le leggi e i regolamenti applicabili e i requisiti contrattuali. | Requisiti GDPR:   * Registro dei trattamenti * Nomine dei responsabili del trattamento * Nomina del DPO * Attestati di formazione per esercitare il ruolo di DPO * Valutazione dei rischi * Valutazione di impatto * Informative agli interessati * Prove di ricezione del consenso da parte degli interessati |
| 5.35 | Independent review of information security | L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e alla sua attuazione, comprese le persone, i processi e le tecnologie, deve essere riesaminato in modo indipendente a intervalli pianificati o quando si verificano cambiamenti significativi. | * Programmi e/o piani di audit indipendenti sul sistema di gestione della sicurezza delle informazioni * Verbali e rapporti di tali audit |
| 5.36 | Compliance with policies, rules and standards for information security | La conformità con la politica di sicurezza delle informazioni dell'organizzazione, le politiche specifiche per argomento, le regole e gli standard deve essere regolarmente riesaminata. |
| 5.37 | Documented operating procedures | Le procedure operative per gli impianti di trattamento delle informazioni sono documentate e messe a disposizione del personale che ne ha bisogno. | Evidenze di come le procedure operative per gli impianti di trattamento delle informazioni sono documentate e messe a disposizione del personale che ne ha bisogno. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6 | ISO 27001 People Controls | | **EVIDENZE E DOCUMENTI DA FORNIRE** | |
| 6.1 | Screening | Control  Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | * Esempi di controlli preliminari sui candidati lavoratori * Accordi contrattuali con i dipendenti relativamente alla sicurezza delle informazioni * Formazione dei dipendenti sulla sicurezza delle informazioni * Politica/procedura di processo disciplinare in caso di contravvenzione alle norme interne di sicurezza delle informazioni * Esempi di richiami al personale relativi alla sicurezza elle informazioni * Documentazione o registrazioni nelle quale si abbia evidenza che i dipendenti siano stati edotti circa le norme di comportamento per la sicurezza delle informazioni * Esempi di accordi di riservatezza con i dipendenti | | |
| 6.2 | Terms and conditions of employment | Control  The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security. |
| 6.3 | Information security awareness, education and training | Control  Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function. |
| 6.4 | Disciplinary process | Control  A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. |
| 6.5 | Responsibilities after termination or change of employment | Control  Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. |
| 6.6 | Confidentiality or non-disclosure agreements | Control  Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. |
| 6.7 | Remote working | Control  Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises. | Descrizione della infrastruttura informatica per garantire la sicurezza durante lo smart working. |
| 6.8 | Information security event reporting | Control  The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. | * Procedure/politiche per segnalare eventi e anomalie all’interno della organizzazione * Evidenze di segnalazione di eventi o anomalie |

|  |  |  |  |
| --- | --- | --- | --- |
| 7 | ISO 27001 Physical Controls | | **EVIDENZE E DOCUMENTI DA FORNIRE** |
| 7.1 | Physical security perimeters | Control  Security perimeters shall be defined and used to protect areas that contain information and other associated assets. | * Descrizione del perimetro di sicurezza a cui si applica il sistema di gestione * Descrizione dei Metodi, strumenti tecnologie di controllo dell’accesso fisico * Descrizione dei Sistemi e/o metodi di Monitoraggio interno degli ambienti contro personale non autorizzato * Evidenze di protezione contro eventi ambientali (incendio, allagamento) * Se presenti, indicare quali sono le zone sicure in cui è possibile continuare a lavorare in caso di eventi malevoli * Screen shot di ciò che viene inquadrato dalle telecamere di sicurezza. * Screen shot del pannello di raccolta degli allarmi sulle minacce fisiche( intrusioni, movimenti, temperatura, umidità) |
| 7.2 | Physical entry | Control  Secure areas shall be protected by appropriate entry Controls and access points. |
| 7.3 | Securing offices, rooms and fa- cilities | Control  Physical security for offices, rooms and facilities shall be designed and implemented. |
| 7.4 | Physical security monitoring | Control  Premises shall be continuously monitored for unauthorized physical access. |
| 7.5 | Protecting against physical and environmental threats | Control  Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. |
| 7.6 | Working in secure areas | Control  Security measures for working in secure areas shall be designed and implemented. |
| 7.7 | Clear desk and clear screen | Control  Clear desk rules for papers and removable Storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. | Procedure per la messa in sicurezza dei device quando non presidiati (es. password di screen saver), pulizia delle scrivanie da documenti classificati |
| 7.8 | Equipment siting and protection | Control  Equipment shall be sited securely and protected. | * Procedure e sistemi di protezione delle attrezzature e dei device mobili (portatili e cellulari) * Screenshot delle applicazioni di asset monitoring e management che controllano i dispositivi portatili e mobili da remoto. |
| 7.9 | Security of assets off-premises | Control  Off-site assets shall be protected. |
| 7.10 | Storage media | Control  Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements. | * Procedura di dismissione degli hard disks e dei dispositivi di memorizzazione * Sistemi di protezione da blackout e picchi di corrente * Caratteristiche di sicurezza dei cavi dati * Rapporti di monitoraggio di manutenzione dei PC, Hardisk etc. * Screen shot delle applicazioni di controllo vita degli HD |
| 7.11 | Supporting Utilities | Control  Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting Utilities. |
| 7.12 | Cabling security | Control  Cables carrying power, data or supporting information Services shall be protected from interception, interference or damage. |
| 7.13 | Equipment maintenance | Control  Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. |
| 7.14 | Secure disposal or re-use of equipment | Control  Items of equipment containing Storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8 | ISO 27001 Technological controls | | **EVIDENZE E DOCUMENTI DA FORNIRE** |
| 8.1 | User end point devices | Control  Information stored on, processed by or accessible via user end point devices shall be protected. | * Procedura/politica di protezione dei dispositivi endpoint * Esempi di protezione degli endpoint * Procedura di assegnazione degli accessi * Esempi di assegnazione di privilegi   Screenshot: di antivirus e firewall a protezione degli end point |
| 8.2 | Privileged access rights | Control  The allocation and use of privileged access rights shall be restricted and managed. |
| 8.3 | Information access restriction | Control  Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. |
| 8.4 | Access to source code | Control  Read and write access to source code, development tools and software libraries shall be appropriately managed. | * Procedura per L'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software deve essere gestito in modo appropriato. * Nominativi degli sviluppatori con tali privilegi |
| 8.5 | Secure authentication | Control  Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. | Descrizione della tecnologia e delle procedure per l’autenticazione sicura  Descrizione deli sistemi di Capacity Management   * Descrizione dei sistemi antivirus e firewall e di sicurezza delle informaizoni * Esempi di scansioni antivirus * Rapporti di penetration test * Rapporti di vulnerability assesment   Screenshot: di antivirus e firewall a protezione del server |
| 8.6 | Capacity management | Control  The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. |
| 8.7 | Protection against malware | Control  Protection against malware shall be implemented and supported by appropriate user awareness. |
| 8.8 | Management of technical vul- nerabilities | Control  Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. |
| 8.9 | Configuration management | Control  Configurations, including security configurations, of hardware, software, Services and networks shall be established, documented, implemented, monitored and reviewed. |
| 8.10 | Information deletion | Control  Information stored in information systems, devices or in any other Storage media shall be deleted when no longer required. | * Procedura, politica, Descrizione dei sistemi di cancellazione sicura di dati non più necessari. * Politica di mascheramento dei dati * Descrizione delle Misure di prevenzione contro la fuga di dati * Screenswhot: di processo di formattazione a basso livello |
| 8.11 | Data masking | Control  Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. |
| 8.12 | Data leakage prevention | Control  Data leakage prevention measures shall be applied to systems, net-works and any other devices that process, store or transmit sensitive information. |
| 8.13 | Information backup | Control  Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic specific policy on backup. | * Politiche/procedure di backup * Screenshot di Log di backup |
| 8.14 | Redundancy of information processing facilities | Control  Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. | * Descrizione dei programmi che raccolgono i logo di attività, eccezioni, guasti e altri eventi rilevanti devono essere prodotti, archiviati, protetti e analizzati. * Screenshot di log di eventi |
| 8.15 | Logging | Control  Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. |
| 8.16 | Monitoring activities | Control  Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. |
| 8.17 | Clock synchronization | Control  The clocks of information processing systems used by the organization shall be synchronized to approved time sources. | Descrizione di sistema di Clock synchronization   * Screen shot Clock synchronization |
| 8.18 | Use of privileged utility programs | Control  The use of utility programs that can be capable of overriding System and application Controls shall be restricted and tightly controlled. | Procedura e sistemi di controllo della limitazione d’uso di programmi di utilità che possono essere in grado di ignorare i controlli del sistema e delle applicazioni deve essere limitato e strettamente controllato.   * Screenshot di schermata di impostazioni di sicurezza (es: web filtering; disabilitazione usb, attivazione bitlocker). |
| 8.19 | Installation of software on operational systems | Control  Procedures and measures shall be implemented to securely manage software installation on operational systems. | Procedure e misure per gestire in modo sicuro l'installazione del software sui sistemi operativi |
| 8.20 | Networks security | Control  Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. | * Descrizione dei sistemi firewall * Evidenze di SLA con clienti e fornitori e meccanismi/strumenti a garanzia * Evidenze di come I gruppi di servizi informativi, gli utenti e i sistemi di informazione sono separati nelle reti dell'organizzazione * Sistemi e politiche di web filtering (screen shot) * Gestione della crittografia e delle chiavi crittogfrafiche * Screen shot delle applicazione di monitoraggio della rete |
| 8.21 | Security of network Services | Control  Security mechanisms, service levels and service requirements of network Services shall be identified, implemented and monitored. |
| 8.22 | Segregationof networks | Control  Groups of information Services, users and information systems shall be segregated in the organization’s networks. |
| 8.23 | Web filtering | Control  Access to external websites shall be managed to reduce exposure to malicious content. |
| 8.24 | Use of cryptography | Control  Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. |
| 8.25 | Secure development life cycle | Control  Rules for the secure development of software and systems shall be established and applied. | * Procedure e politiche di sviluppo sicuro * Documentazione dei requisiti di sicurezza del codice * Esempi Test di sicurezza del codice sviluppato * Descrizione della separazione sviluppo, collaudo e produzione * Screen shot dei risultati delle applicazioni utilizzate per fare il code security check testthreat |
| 8.26 | Application security requirements | Control  Information security requirements shall be identified, specified and approved when developing or acquiring applications. |
| 8.27 | Secure System architecture and engineering principles | Control  Principles for engineering secure systems shall be established, documented, maintained and applied to any information System development activities. |
| 8.28 | Secure coding | Control  Secure coding principles shall be applied to software development. |
| 8.29 | Security testing in development and acceptance | Control  Security testing processes shall be defined and implemented in the development life cycle. |
| 8.30 | Outsourced development | Control  The organization shall direct, monitor and review the activities related to outsourced system development. |
| 8.31 | Separation of development, test and production environments | Control  Development, testing and production environments shall be separated and secured. |
| 8.32 | Change management | Control  Changes to information processing facilities and information systems shall be subject to change management procedures. | Procedura di gestione delle modifiche apportate agli impianti e ai sistemi di informazione. |
| 8.33 | Test information | Control  Test information shall be appropriately selected, protected and managed. | * Sistemi di protezione dei dati quando utilizzati nei processi di test e di audit * Verbali/rapporti di test |
| 8.34 | Protection of information systems during audit testing | Control  Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. |