QM-03 Bezpečnostní politika

QM-03 Política de Seguridad

Viatep Iberica

Obsah

1 Bezpečnost informací – Úvod/ Seguridad de la información - Introducción

VIATEP IBERICA se specializuje na vývoj a výrobu čistících rohoží a čistících zón pro všechny zákazníky – organizace, firmy, soukromé osoby, státní správu, atd. Bezpečnost informací je charakterizována jako zachování důvěrnosti, integrity a dostupnosti informací. Důvěrnost znamená zajištění skutečnosti, že informace je přístupná jen těm uživatelům, kteří jsou oprávněni k ní mít přístup. Integrita představuje zabezpečení přesnosti a kompletnosti informací a metod jejich zpracování. Dostupnost znamená zajištění, že jsou informace a s nimi spojená aktiva uživatelům přístupná v době, kdy je potřebují. Tato Bezpečnostní politika je základním řídícím dokumentem, který vyjadřuje postoj vedení k zajištění bezpečnosti informací.

VIATEP IBERICA está especializada en el desarrollo y producción de felpudos y zonas de limpieza para todos los clientes: organizaciones, empresas, particulares, administración estatal, etc. La seguridad de la información se caracteriza por mantener la confidencialidad, integridad y disponibilidad de la información. Confidencialidad significa garantizar que la información sea accesible solo para aquellos usuarios que están autorizados a tener acceso a ella. Integridad significa garantizar la exactitud y la integridad de la información y sus métodos de procesamiento. Disponibilidad significa garantizar que la información y los activos asociados sean accesibles para los usuarios cuando los necesiten. Esta Política de Seguridad es el documento rector básico que expresa la posición de la dirección para garantizar la seguridad de la información.

2 Cíle systému bezpečnosti informací / Objetivos del sistema de seguridad de la información

Cílem bezpečnosti informací je zajistit ochranu využívaných informací a zabránit neoprávněnému nakládání s informacemi ve všech formách jejich výskytu. Zejména je třeba zajistit dostupnost informačních aktiv jen oprávněným osobám, správnost a kompletnost informací, důvěrnost a bezpečnost jejich zpracování a ochranu informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám anebo šíření.
Záměrem vedení je udržovat přiměřenou ochranu informačních aktiv v souladu s právními předpisy České republiky a Evropské unie, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na externí subjekty.

El objetivo de la seguridad de la información es garantizar la protección de la información utilizada y evitar el manejo no autorizado de la información en todas sus formas. En particular, es necesario garantizar la disponibilidad de los activos de información solo para las personas autorizadas, la exactitud e integridad de la información, la confidencialidad y seguridad de su procesamiento y la protección de la información contra la destrucción accidental o no autorizada o la pérdida accidental, contra el acceso no autorizado, cambios o difusión. La intención de la gerencia es mantener una protección adecuada de los activos de información de acuerdo con las leyes de la República Checa y la Unión Europea, incluso en los casos en que la responsabilidad del procesamiento de la información se haya transferido a entidades externas.

3 Rozsah a význam systému bezpečnosti informací v/ El alcance e importancia del sistema de seguridad de la información en VIATEP IBERICA

Systém řízení bezpečnosti informací se vztahuje na oblasti - Návrh a vývoj, výroba, montáž a prodej rohoží, vstupních čistících zón a doplňků.
Hlavní činnosti související s bezpečností informací jsou zajišťovány v areálu sídla firmy, kde je zároveň management i výroba: VIATEP IBÉRICA 2012, S.L., C/. Del Tejar, 24 Pol. Ind. Los Salmueros - 28978 Cubas de la Sagra (Madrid)

ISMS zahrnuje:

1. osobní informace vztahující se k zaměstnancům VIATEP IBERICA
2. informace o smluvních partnerech VIATEP IBERICA
3. informace o dodavatelích VIATEP IBERICA
4. informace o zákaznících VIATEP IBERICA
5. informace obchodní, právní a smluvní
6. komunikace všech zmíněných účastníků interní, externí včetně komunikace se státní správou a ostatních oprávněných orgánů
7. IT infrastrukturu VIATEP IBERICA (servery, síť, notebooky, stanice, komunikační a zabezpečovací prostředky, kamerové systémy, atd.)

Všichni uživatelé informačního systému VIATEP IBERICA v rámci dodržování bezpečnosti informací zajišťují:

- dodržování ochrany osobních údajů všech kategorií u všech zákazníků, dodavatelů, zaměstnanců, atd.
- dodržování ochrany obchodního tajemství a obsahu smluv obchodně závazkových vztahů, k nimž se společnost VIATEP IBERICA v uzavřených smlouvách zavázala;
- dodržování ochrany skutečností, jejichž zneužití by mohlo vést k ohrožení života, zdraví, majetku, životního prostředí nebo podnikatelského zájmu společnost VIATEP IBERICA
- dodržování ochrany práv a svobod jednotlivců, zejména právo na soukromí, podle Listiny základních práv a svobod;
- dodržování ochrany listovního tajemství
- dodržování ochrany prostředků a dat pro vytváření zaručeného elektronického podpisu podle zvláštního zákona;
- dodržování ochrany záležitostí, které jsou předmětem bankovního tajemství podle zvláštního zákona.

El sistema de gestión de seguridad de la información cubre las áreas - Diseño y desarrollo, producción, montaje y venta de alfombras, zonas de limpieza de entrada y accesorios.
Las principales actividades relacionadas con la seguridad de la información se prestan en la zona de la sede social de la empresa, donde se encuentran tanto la dirección como la producción: VIATEP IBÉRICA 2012, SL, C/. Del Tejar, 24 Pol. Indio. Los Salmueros - 28978 Cubas de la Sagra (Madrid)

SGSI incluye:

1. datos personales relativos a los empleados de VIATEP IBERICA
2. información sobre los socios contractuales de VIATEP IBERICA
3. información sobre proveedores de VIATEP IBERICA
4. información sobre los clientes de VIATEP IBERICA
5. información comercial, legal y contractual
6. comunicación de todos los participantes mencionados, internos y externos, incluida la comunicación con la administración estatal y otros organismos autorizados
7. Infraestructura TI de VIATEP IBERICA (servidores, red, portátiles, estaciones, dispositivos de comunicación y seguridad, sistemas de cámaras, etc.)

Todos los usuarios del sistema de información de VIATEP IBERICA, en cumplimiento de la seguridad de la información, garantizan:

- cumplimiento de la protección de datos personales de todas las categorías para todos los clientes, proveedores, empleados, etc.

- el cumplimiento de la protección de los secretos empresariales y del contenido de los contratos de las obligaciones comerciales a las que VIATEP IBERICA se ha comprometido en los contratos celebrados;
- el cumplimiento de la protección de los hechos, cuyo uso indebido podría suponer una amenaza para la vida, la salud, los bienes, el medio ambiente o el interés empresarial de VIATEP IBERICA
- el cumplimiento de la protección de los derechos y libertades de las personas, en especial el derecho a la intimidad, según la Carta de los Derechos y Libertades Fundamentales;
- cumplimiento de la protección del secreto de las cartas
- el cumplimiento de la protección de medios y datos para la creación de una firma electrónica garantizada según una ley especial;
- el cumplimiento de la protección de los asuntos que sean objeto del secreto bancario conforme a una ley especial.

4 Prohlášení vedení VIATEP IBERICA/ Comunicado de la dirección de VIATEP IBERICA

Vedení společnosti VIATEP IBERICA si uvědomuje, že vysoká úroveň využívání informačních a komunikačních technologií, jak v rámci zpracování informací uvnitř VIATEP IBERICA, tak i v rámci komunikace se zákazníky a partnery také přináší rizika. Tato „Bezpečnostní politika VIATEP IBERICA“ je základní normou, kterou vedení vydává pro zajištění bezpečného a efektivního řízení bezpečnosti aktiv a informací. Tato bezpečnostní politika je závazná pro všechny osoby i organizace, jejichž činnost se jakýmkoli způsobem dotýká společnosti VIATEP IBERICA. Účelem bezpečnostní politiky je formulace jasné a závazné koncepce řešení informační bezpečnosti a definice základních přístupů při budování informační bezpečnosti ve společnosti VIATEP IBERICA. Bezpečnostní politika vytváří základ pro tvorbu vnitřních norem - bezpečnostních zásad a postupů, bezpečnostních standardů a směrnic a definuje zásady chování všech účastníků – tj. uživatelů, vedoucích pracovníků, externích spolupracovníků, správců i třetích stran.
Vedení VIATEP IBERICA deklaruje bezpečnostní politikou svou strategii trvalého zajišťování systému bezpečnosti informací jako nedílné součásti všech řídicích procesů.
Bezpečnostní principy a zásady deklarované touto bezpečnostní politikou budou tak postupně rozpracovávány a zpřesňovány podle konkrétních podmínek, požadavků a potřeb jednotlivých zákazníků, dodavatelů, úřadů a jejich informačních systémů.

La dirección de VIATEP IBERICA es consciente de que el alto nivel de uso de las tecnologías de la información y la comunicación, tanto en el tratamiento de la información dentro de VIATEP IBERICA como en la comunicación con los clientes y socios, también conlleva riesgos. Esta “Política de Seguridad de VIATEP IBERICA” es la norma básica emitida por la dirección para garantizar la gestión segura y eficaz de la seguridad de los activos y de la información. Esta política de seguridad es vinculante para todas las personas y organizaciones cuyas actividades afecten a VIATEP IBERICA de cualquier forma.
El objetivo de la política de seguridad es la formulación de un concepto claro y vinculante de soluciones de seguridad de la información y la definición de enfoques básicos en la construcción de la seguridad de la información en VIATEP IBERICA. La política de seguridad crea la base para la creación de estándares internos - principios y procedimientos de seguridad, estándares y directrices de seguridad y define los principios de comportamiento de todos los participantes - es decir, usuarios, ejecutivos, colaboradores externos, administradores y terceros.
La dirección de VIATEP IBERICA declara en la política de seguridad su estrategia de velar permanentemente por el sistema de seguridad de la información como parte integrante de todos los procesos de gestión.

Los principios de seguridad y los principios declarados en esta política de seguridad se desarrollarán y perfeccionarán gradualmente de acuerdo con las condiciones, requisitos y necesidades específicas de los clientes, proveedores, autoridades y sus sistemas de información

5 Bezpečnostní tým / Equipo de seguridad

V rámci stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů byl stanoven „Bezpečnostní tým“ jako vrcholný orgán v oblasti systému bezpečnosti informací.

Bezpečnostní tým:

- stanovuje způsob zajištění bezpečnosti informací
- navrhuje a prosazuje zavedení bezpečnostních opatření do praxe
- vyhodnocuje vzdělávání zaměstnanců v oblasti bezpečnosti informací
- zajišťuje nezávislé revize bezpečnosti informací
- provádí přezkoumávání dokumentů souvisejících s bezpečností informací z hlediska jejich použitelnosti a aktuálnosti

Členy bezpečnostního týmu jmenuje a odvolává jednatel.
Bezpečnostní tým se schází podle potřeby, nejméně však 4x ročně.
Bezpečnostní tým je složen z následujících osob:

- Bezpečnostní manažer / manažer ISŘ / Jednatel společnosti
- Správce IT
- Člen týmu - většinový vlastník / jednatel GAPA MB

Bezpečnostní manažer:

- koordinuje činnost Bezpečnostního týmu,
- prosazuje Bezpečnostní politiku,
- sleduje dodržování bezpečnostních opatření ve všech oblastech informační bezpečnosti,
- navrhuje změny politiky, směrnic a navazujících dokumentů a dohlíží na provádění změn,
- řeší bezpečnostní události
- zajišťuje kontakt se státní správou a dalšími potřebnými autoritami
- koordinuje školení zaměstnanců v oblasti informační bezpečnosti,
- plánuje a provádí nezávislé revize bezpečnosti informací
- připomínkuje aplikaci bezpečnostních opatření z hlediska integrovaného systému managementu,
- řeší bezpečnostní události v oblasti systému integrovaného managementu
- sleduje dodržování bezpečnostních opatření ve všech oblastech systému integrovaného managementu
- spolupracuje na disciplinárním řízení

Správce IT:

- připomínkuje aplikaci bezpečnostních opatření z hlediska použitých IT technologií,
- řeší bezpečnostní události v oblasti IT
- sleduje dodržování bezpečnostních opatření ve všech oblastech informační bezpečnosti
- navrhuje a řeší technická bezpečnostní opatření v oblasti IT
- spolupracuje na disciplinárním řízení

Člen týmu:

- připomínkuje aplikaci bezpečnostních opatření z hlediska použitých technologií,
- řeší bezpečnostní události
- sleduje dodržování bezpečnostních opatření ve všech oblastech informační bezpečnosti
- schvaluje technická a systémová bezpečnostní opatření

- spolupracuje na disciplinárním řízení

En el marco de la determinación de responsabilidades generales y específicas para el área de gestión de la seguridad de la información, incluyendo el reporte de incidentes de seguridad, se constituyó el "Equipo de Seguridad" como máxima autoridad en el área del sistema de seguridad de la información.

Equipo de seguridad:

- determina el método para garantizar la seguridad de la información
- propone y promueve la implementación de medidas de seguridad en la práctica
- evalúa la formación de los empleados en el ámbito de la seguridad de la información
- proporciona revisiones independientes de la seguridad de la información
- revisa los documentos relacionados con la seguridad de la información desde el punto de vista de su aplicabilidad y actualidad

Los miembros del equipo de seguridad son designados y destituidos por el ejecutivo.
El equipo de seguridad se reúne según sea necesario, pero al menos 4 veces al año.
El equipo de seguridad está formado por las siguientes personas:

- Gerente de seguridad / Gerente ISŘ / Ejecutivo de empresa
- Administrador IT
- Miembro del equipo - propietario mayoritario / ejecutivo de GAPA MB

Gerente de seguridad:

- coordina las actividades del Equipo de Seguridad,
- hace cumplir la Política de Seguridad,
- supervisa el cumplimiento de las medidas de seguridad en todos los ámbitos de la seguridad de la información,
- propone cambios a la política, las directrices y los documentos de seguimiento y supervisa la implementación de los cambios,
- maneja incidentes de seguridad
- asegura el contacto con la administración estatal y otras autoridades necesarias
- coordina la formación de los empleados en el campo de la seguridad de la información,
- planifica y realiza auditorías independientes de seguridad de la información
- recuerda la aplicación de medidas de seguridad desde el punto de vista del sistema integrado de gestión,
- resuelve eventos de seguridad en el área del sistema de gestión integrado
- supervisa el cumplimiento de las medidas de seguridad en todos los ámbitos del sistema integrado de gestión
- coopera en procedimientos disciplinarios

Administrador IT:

- recuerda la aplicación de medidas de seguridad en cuanto a las tecnologías informáticas utilizadas,
- resuelve eventos de seguridad en el campo de TI
- supervisa el cumplimiento de las medidas de seguridad en todos los ámbitos de la seguridad de la información
- diseña y resuelve medidas técnicas de seguridad en el ámbito de las TI
- coopera en procedimientos disciplinarios

Miembro del equipo:

- recuerda la aplicación de medidas de seguridad en cuanto a las tecnologías utilizadas,
- maneja incidentes de seguridad
- supervisa el cumplimiento de las medidas de seguridad en todos los ámbitos de la seguridad de la información

- aprueba las medidas técnicas y de seguridad del sistema
- coopera en procedimientos disciplinarios

6 Přístup k hodnocení a řízení rizik/ Enfoque de la evaluación y gestión de riesgos

K identifikaci aktiv, hrozeb a hodnocení rizik VIATEP IBERICA využívá zejména metodik popsaných v ISO/IEC 27005. Spolupráce na úrovni bezpečnostního týmu vyústila k postupnému zpracování registru rizik ISMS, který obsahuje jednotlivá aktiva a jejich typy, definuje vlastníky aktiv a zranitelnosti. Následně uvádí příslušné hrozby a s nimi spojené dopady. Výsledek je hodnocení jednotlivých rizik dle stanovené kvalitativní metodiky uvedené v příloze registru rizik. Na základě takto zpracovaného registru a informací, které byly k dispozici k identifikaci možných opatření včetně normativních podkladů byla stanovena příslušná opatření k řízení jednotlivých rizik. Vyhodnocení řízení a efektivnosti je zajišťováno bezpečnostním týmem v rámci přezkoumání vedením jedenkrát ročně.

Para identificar activos, amenazas y evaluar riesgos, VIATEP IBERICA utiliza principalmente las metodologías descritas en ISO/IEC 27005. La cooperación a nivel del equipo de seguridad resultó en el procesamiento gradual del registro de riesgos del SGSI, que contiene activos individuales y sus tipos, define los propietarios de activos y vulnerabilidades. Posteriormente, enumera las respectivas amenazas y sus impactos asociados. El resultado es una evaluación de los riesgos individuales de acuerdo con la metodología cualitativa establecida que se detalla en el anexo del registro de riesgos. Sobre la base del registro procesado de esta manera y la información que estaba disponible para identificar posibles medidas, incluidos los documentos normativos, se determinaron las medidas apropiadas para gestionar los riesgos individuales. El equipo de seguridad proporciona una evaluación de la gestión y la eficacia como parte de una revisión de la gestión una vez al año.

7 Hlavní opatření a základní bezpečnostní zásady / Principales precauciones y principios básicos de seguridad

V rámci celé firmy VIATEP IBERICA musí být zabezpečena hlavně opatření pro:

- pravidelné monitorování a vyhodnocování bezpečnostních rizik a incidentů – musí být přijímána měřitelná opatření vedoucí k omezení vlivu tak, aby docházelo ke zlepšování úrovně bezpečnosti a aby náklady na realizaci opatření odpovídaly ceně chráněných informací,
- zabezpečení požadavků vyplývajících ze smluvních závazků, obecně závazných právních předpisů a nařízení - musí být veden přehled těchto požadavků a odpovědnost za jejich plnění,
- zabezpečení včasné dostupnosti informací - doba kritické dostupnosti informací musí být stanovena, a to v souladu s jejich významem,
- zamezení nežádoucí modifikace informací - musí být určen rozsah kontroly a opatření k zamezení modifikace,
- případné zneužití nebo ztráty informací - musí být definována odpovědnost a způsob ochrany při přístupu k informacím a do prostor kde se nachází informační hodnoty,
- zabezpečení výběru zaměstnanců/spolupracovníků z hlediska ochrany informací, se zaměstnanci/spolupracovníky VIATEP IBERICA provádět pravidelná školení v oblasti politiky bezpečnosti informací,
- pro zajištění použitelnosti a účinnosti politiky bezpečnosti informací je ze strany vedení VIATEP IBERICA a bezpečnostním týmem tato politika pravidelně přezkoumávána a monitorována.

Základní bezpečnostní zásady VIATEP IBERICA vycházejí z těchto požadavků:

- dodržení právních předpisů, závazných norem, vnitřních předpisů a smluvních požadavků,
- dosažení stanoveného cíle – provedenými opatřeními zabezpečit ochranu informací,
- provedená bezpečnostní opatření nesmí omezovat standardní provoz VIATEP IBERICA,

- náklady spojené s přijetím opatření na snížení rizik musí být v rovnováze s případnými škodami způsobenými selháním bezpečnosti.

Dentro de toda la empresa VIATEP IBERICA, medidas para:

- monitoreo y evaluación regulares de los riesgos e incidentes de seguridad: se deben tomar medidas medibles para limitar el impacto para que el nivel de seguridad mejore y los costos de implementación de las medidas correspondan al precio de la información protegida,
- asegurar los requisitos que surgen de las obligaciones contractuales, generalmente las normas y reglamentos legales vinculantes: se debe mantener una descripción general de estos requisitos y la responsabilidad de su cumplimiento,
- garantizar la disponibilidad oportuna de la información: el momento de la disponibilidad crítica de la información debe determinarse de acuerdo con su importancia,
- prevención de la modificación no deseada de la información: se debe determinar el alcance del control y las medidas para evitar la modificación,
- posible uso indebido o pérdida de información: se debe definir la responsabilidad y el método de protección al acceder a la información y las áreas donde se encuentran los valores de la información,
- asegurar la selección de empleados/colaboradores desde el punto de vista de la protección de la información, realizar capacitaciones regulares en el campo de la política de seguridad de la información con los empleados/colaboradores de VIATEP IBERICA,
- para asegurar la aplicabilidad y eficacia de la política de seguridad de la información, esta política es revisada y monitoreada periódicamente por la dirección de VIATEP IBERICA y el equipo de seguridad.

Principios básicos de seguridad de VIATEP IBERICA se basan en los siguientes requisitos:

- el cumplimiento de las normas legales, las normas vinculantes, los reglamentos internos y los requisitos contractuales,
- logro del objetivo establecido: garantizar la protección de la información a través de las medidas implementadas,
- las medidas de seguridad implementadas no deben limitar el normal funcionamiento de VIATEP IBERICA,

los costos asociados con la adopción de medidas para reducir los riesgos deben equilibrarse con los daños potenciales causados por una falla de seguridad.

7.1 Organizace bezpečnosti a přenosu informací/ Organización de la seguridad y transferencia de información

Základní odpovědnost za řízení a koordinaci bezpečnosti informací má Bezpečnostní tým.

Vedoucí pracovníci odpovídají za správnost, využitelnost a ochranu informací v rámci své působnosti, stanovují procesy zpracování informací.

Všichni uživatelé informačního systému jsou povinni respektovat pravidla definovaná dokumentem Politika integrovaného systému VIATEP IBERICA (touto bezpečnostní politikou) a Manuálem uživatele IT. Veškeré odchylky od definovaných pravidel jsou povinni neprodleně oznámit Manažerovi bezpečnosti informací.

Přístup k informacím a jiným informačním aktivům pro externí subjekty je možný pouze na základě smluvního ujednání, které musí obsahovat závazek zajišťovat ochranu informací a mlčenlivost. Přenos informací v rámci interní i externí komunikace je zajišťován způsobem a komunikačním vybavením v souladu s postupy stanovenými správcem IT/bezpečnostním týmem. Realizace je rozpracována ve směrnici pro správce IT.

Jsou prováděny pravidelné kontroly informačního systému za účelem zjištění zda jsou dodržována platná pravidla a zásady pro bezpečnost Manažerem bezpečnosti informací ve spolupráci s externími subjekty.

El Equipo de seguridad tiene la responsabilidad principal de administrar y coordinar la seguridad de la información.

Los administradores son responsables de la corrección, usabilidad y protección de la información dentro de su ámbito, establecen procesos de procesamiento de información.

Todos los usuarios del sistema de información están obligados a respetar las normas definidas en el documento de Política del Sistema Integrado de VIATEP IBERICA (la presente política de seguridad) y en el Manual de Usuario de TI. Todas las desviaciones de las reglas definidas deben ser reportadas inmediatamente al Gerente de Seguridad de la Información.

El acceso a la información y otros activos de información para entidades externas solo es posible sobre la base de un acuerdo contractual, que debe incluir la obligación de garantizar la protección y confidencialidad de la información. La transferencia de información como parte de la comunicación interna y externa está asegurada por el método y el equipo de comunicación de acuerdo con los procedimientos establecidos por el administrador de TI/equipo de seguridad. La implementación se detalla en la directiva para administradores de TI.

Se llevan a cabo verificaciones regulares del sistema de información para determinar si el Gerente de Seguridad de la Información está siguiendo las reglas y principios válidos para la seguridad en cooperación con entidades externas.

7.2 Řízení aktiv a klasifikace/ Gestión y clasificación de activos

Je zavedena a udržována evidence aktiv (viz QR-06 Registr aktiv a hodnocení rizik ISMS) u nichž je určen vlastník a jednoznačně stanovena odpovědnost za dodržování povinností při jejich zpracování, shromažďování a uchovávání v souladu s platnými předpisy.

Informační aktiva jsou klasifikována čímž se určuje způsob zacházení s informacemi s ohledem na jejich ochranu z hlediska důvěrnosti. Klasifikaci stanoví vlastníci informačních aktiv nebo vlastníci procesů, kteří odpovídají za periodické přezkoumávání této klasifikace a její aktualizaci, dle postupu pro řízení dokumentů.

Uživatelé informačního systému si musí být vědomi své odpovědnosti při nakládání s informacemi a dalšími aktivy.

Se establece y lleva un registro de activos (ver QR-06 Registro de activos y evaluación de riesgos SGSI) para el cual se determina el titular y se establece claramente la responsabilidad del cumplimiento de las obligaciones durante su procesamiento, acopio y almacenamiento de acuerdo con la normatividad aplicable.

Los activos de información se clasifican, lo que determina cómo se maneja la información con respecto a su protección de la confidencialidad. La clasificación es determinada por los propietarios de los activos de información o propietarios de los procesos, quienes son los responsables de revisar periódicamente esta clasificación y actualizarla, de acuerdo con el procedimiento de gestión documental.

Los usuarios del sistema de información deben ser conscientes de sus responsabilidades al manejar la información y otros activos.

7.3 Personální bezpečnost/ Seguridad personal

Záměrem je zajištění vhodných postupů v rámci přijímacího i výstupního řízení, zajistit povědomí zaměstnanců o bezpečnosti informací a být připraven řešit všechny incidenty a uplatňovat principy disciplinárního řízení v případech nedodržení zásad bezpečnosti informací.

Zaměstnanci/spolupracovníci VIATEP IBERICA či ostatní externí subjekty jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění svých úkolů a činností nebo v přímé souvislosti s nimi a tato povinnost trvá i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak.

La intención es asegurar procedimientos adecuados dentro de los procedimientos de admisión y salida, para asegurar la conciencia de los empleados sobre la seguridad de la información y estar preparados para resolver todos los incidentes y aplicar los principios de procedimientos disciplinarios en casos de incumplimiento de los principios de seguridad de la información.

Los empleados/compañeros de VIATEP IBERICA o de otras entidades externas están obligados a guardar confidencialidad sobre los hechos de los que tengan conocimiento en el ejercicio de sus funciones y actividades o en relación directa con ellas, y esta obligación subsiste incluso después de la terminación de la relación laboral. relación, salvo disposición legal especial en contrario.

7.4 Fyzická bezpečnost a bezpečnost prostředí/ Seguridad física y ambiental

Záměr VIATEP IBERICA je předcházet neoprávněnému a neautorizovanému přístupu k informacím, poškození a narušení informací. Toto je zajištěno fyzickou ochranou informací a prostor, ve kterém se informace nacházejí, vymezením a využíváním zabezpečených oblastí s prostředky IT, zahrnujících kontrolu vstupu a upřesněním způsobu práce osob v těchto oblastech, zabezpečením kanceláří, místností a zařízení, ochranou proti hrozbám působícím z vnějšího prostředí, zejména tam, kde se informace nacházejí, zpracovávají a uchovávají.

Stanovení režimu vstupu a výstupu osob a zajištění zabezpečených oblastí s prostředky IT včetně definování fyzického bezpečnostního perimetru zajišťuje Systémový technik ve spolupráci s Manažerem bezpečnosti informací.

Fyzické prostředky pro vstup do perimetru VIATEP IBERICA jsou řízeny a evidovány v QR-11 Evidence klíčů, čipů a ovladačů. Pro ochranu prostor s přístupem veřejnosti jsou využívány kamerové systémy.

La intención de VIATEP IBERICA es evitar el acceso no autorizado y no autorizado a la información, el daño y la interrupción de la información. Esto se asegura mediante la protección física de la información y del espacio en el que se encuentra la información, la definición y uso de áreas seguras con recursos informáticos, incluyendo el control de acceso y la especificación de la forma de trabajo de las personas en estas áreas, la seguridad de las oficinas, salas y equipos, protección contra amenazas que actúan desde el entorno exterior, especialmente donde se localiza, procesa y almacena la información.

La determinación del modo de entrada y salida de personas y la protección de áreas seguras con recursos de TI, incluida la definición del perímetro de seguridad física, está a cargo del ingeniero de sistemas en cooperación con el gerente de seguridad de la información.

Los medios físicos de entrada al perímetro de VIATEP IBERICA se gestionan y registran en el QR-11 Registro de llaves, chips y controladores. Los sistemas de cámaras se utilizan para proteger las áreas de acceso público.

7.5 Řízení komunikací a řízení provozu/ Gestión del tráfico y gestión del tráfico

VIATEP IBERICA zajišťuje správný a bezpečný provoz prostředků pro zpracování informací, minimalizuje riziko selhání systému, chrání integritu a dostupnost informačních aktiv a informačního systému, chrání důvěrnost informačních aktiv a zajišťuje ochranu počítačových sítí a prostředků pro komunikaci a zpracování dat. Zásahy a změny do informačních systémů musí být před implementací řádně otestovány a schváleny bezpečnostním týmem. Rozhodnutí o nasazení nových verzí jsou činěna na základě hodnocení možných rizik v porovnání s potřebami a přínosy provedených změn. Jestliže má změna možný dopad do oblasti osobních údajů, je třeba zajistit shodu s příslušnou legislativou.

Na všech prvcích informačního systému je zajištěna ochrana před viry a škodlivými mobilními kódy. Informační aktiva jsou zajištěna příslušnými zálohami proti ztrátě.

VIATEP IBERICA vela por el correcto y seguro funcionamiento de los medios de tratamiento de la información, minimiza el riesgo de fallo del sistema, protege la integridad y disponibilidad de los activos de información y del sistema de información, protege la confidencialidad de los activos de información y asegura la protección de las redes informáticas y de los medios de comunicación y procesamiento de datos. Las intervenciones y los cambios en los sistemas de información deben ser debidamente probados y aprobados por el equipo de seguridad antes de su implementación. Las decisiones de implementar nuevas versiones se toman en base a una evaluación de los posibles riesgos en comparación con las necesidades y los beneficios de los cambios realizados. Si el cambio tiene un posible impacto en el área de datos personales, es necesario garantizar el cumplimiento de la legislación pertinente.

Todos los elementos del sistema de información están protegidos contra virus y códigos móviles dañinos. Los activos de información están garantizados por depósitos apropiados contra pérdidas.

7.6 Řízení přístupu, práce na dálku a síťové služby/ Control de acceso, teletrabajo y servicios de red

VIATEP IBERICA zajišťuje řízení přístupu k informacím a informačním aktivům, citlivým informacím a osobním údajům tak, aby k nim měli přístup pouze oprávnění uživatelé. Přístupy do informačního systému jsou řízeny na základě přístupových oprávnění, které je řízeno v souladu s klasifikací informačních aktiv a s ohledem na neslučitelnost rolí.

Informační aktiva VIATEP IBERICA jsou chráněna proti neautorizované či náhodné změně, ztrátě a odcizení. V případě správce informačního systému musí být přístupy autorizovány Manažerem bezpečnosti informací.

Přístup k síťovým prvkům je řízen s ohledem na vyloučení rizika neautorizovaného přístupu. Může být povolen pouze na základě odpovídající autorizace. Přistup k systémovým příkazům operačního systému musí být omezen pouze pro správce informačního systému.

Vzdálený přístup do informačního systému je zajištěn tak, aby bylo zabráněno jeho zneužití. Práce na dálku je zajišťována tak, aby byla zajištěna bezpečnost informačního systému.

Správu síťového prostředí, správu síťových zařízení a aplikaci bezpečnostních postupů v síťovém prostředí informačního systému vykonává správce IT.

Politika řízení přístupu, práce na dálku a síťových služeb je dále rozpracována ve směrnicích pro správce a uživatele IT.

VIATEP IBERICA asegura el control de acceso a la información y activos de información, información sensible y datos de carácter personal para que sólo los usuarios autorizados tengan acceso a ellos. El acceso al sistema de información se gestiona en base a autorizaciones de acceso, las cuales se gestionan de acuerdo con la clasificación de los activos de información y en cuanto a la incompatibilidad de roles.

Los activos de información de VIATEP IBERICA están protegidos contra cambios, pérdidas y robos no autorizados o accidentales. En el caso de un administrador del sistema de información, el acceso debe ser autorizado por el Gerente de Seguridad de la Información.

El acceso a los elementos de la red se controla con respecto a la eliminación del riesgo de acceso no autorizado. Sólo se puede permitir con base en la autorización correspondiente. El acceso a los comandos del sistema del sistema operativo debe estar restringido únicamente al administrador del sistema de información.

Se asegura el acceso remoto al sistema de información de forma que se evite su uso indebido. El trabajo remoto se proporciona de tal manera que se garantice la seguridad del sistema de información.

La gestión del entorno de red, la gestión de los dispositivos de red y la aplicación de procedimientos de seguridad en el entorno de red del sistema de información está a cargo del administrador de TI.

Las políticas de control de acceso, teletrabajo y servicios de red se elaboran con más detalle en las directrices para administradores y usuarios de TI.

7.7 Používání mobilních zařízení/ Uso de dispositivos móviles

VIATEP IBERICA používá mobilní komunikační zařízení s přístupem do informačního systému. Přístup k informačnímu systému je zajištěn tak, aby byla zajištěna bezpečnost informačního systému a souvisejících dat. Jsou stanovena bezpečnostní pravidla pro nákup, používání a výměnu mobilních komunikačních zařízení. Aplikace a detailní rozpracování politiky mobilních zařízení je uvedeno ve směrnici pro správce a uživatele IT. Mobilní zařízení jsou přidělována dokumentovaným způsobem a zaměstnanci jsou si vědomi důležitosti dodržování pravidel ve směrnici uživatele IT.

VIATEP IBERICA utiliza un dispositivo de comunicación móvil con acceso al sistema de información. El acceso al sistema de información está garantizado para garantizar la seguridad del sistema de información y los datos relacionados. Se establecen reglas de seguridad para la compra, uso e intercambio de dispositivos de comunicación móvil. La aplicación y elaboración detallada de la política para dispositivos móviles se da en la directiva para administradores y usuarios de TI. Los dispositivos móviles se asignan de manera documentada y los empleados son conscientes de la importancia de seguir las reglas de la directiva de usuarios de TI.

7.8 Vývoj a údržba systémů/ Desarrollo y mantenimiento de sistemas

VIATEP IBERICA zajišťuje bezpečnost informací do celého životního cyklu provozovaných částí informačního systému od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace a změny jsou spojeny se stanovením vhodných bezpečnostních požadavků.

Při změnách informačního systému VIATEP IBERICA, které mohou mít vliv na bezpečnost, jsou prováděny analýzy rizik. Analýzy rizik a audit informačního systému představují způsob kontroly řízení rizik informačního systému. Bez schválení bezpečnostního týmu nesmí být v informačním systému VIATEP IBERICA instalovány a používány žádné informační a komunikační technologie. Tyto musí pocházet z důvěryhodných zdrojů a před nasazením musí být řádně otestovány.

VIATEP IBERICA garantiza la seguridad de la información durante todo el ciclo de vida de las partes operadas del sistema de información, desde la fase de diseño, desarrollo y pruebas hasta la operación y mantenimiento reales. La implementación y los cambios están asociados con el establecimiento de requisitos de seguridad apropiados.

Se realizan análisis de riesgo de cambios en el sistema de información de VIATEP IBERICA que puedan afectar a la seguridad. Los análisis de riesgos y las auditorías de los sistemas de información son una forma de comprobar la gestión de riesgos de los sistemas de información. No se podrán instalar y utilizar tecnologías de la información y la comunicación en el sistema de información de VIATEP IBERICA sin la aprobación del equipo de seguridad. Estos deben provenir de fuentes confiables y deben probarse adecuadamente antes de la implementación.

7.9 Řízení incidentů – neshod bezpečnosti informací/ Gestión de incidentes: incumplimiento de la seguridad de la información

VIATEP IBERICA zajišťuje minimalizaci škod způsobených bezpečnostními incidenty a prevenci před jejím výskytem či opakováním. Bezpečnostní incidenty představují zejména všechna porušení pravidel nakládání s informacemi a příslušnými informačními aktivy VIATEP IBERICA, které musí být řádně vyšetřeny pracovníky s odpovídajícími zkušenostmi a kvalifikací.

Každý uživatel informačního systému je povinen neodkladně nahlásit porušení (či důvodné podezření) bezpečnosti informací prostřednictvím příslušného vedoucího pracovníka Manažerovi bezpečnosti informací, který je odpovědný za jejich evidenci a koordinaci vyšetřování v případě spolupráce s orgány činnými v trestním řízení.

Šetření bezpečnostních incidentů zajišťuje Manažer bezpečnosti a Bezpečnostní tým. Bezpečnostní incidenty jsou evidovány, a jsou pravidelně hodnoceny související hrozby a rizika. Výsledkem je zlepšení prevence výskytu bezpečnostních incidentů a tím zlepšování celého systému bezpečnosti informací.

VIATEP IBERICA vela por la minimización de los daños causados por incidentes de seguridad y la prevención de su ocurrencia o reincidencia. Los incidentes de seguridad representan, en particular, todas las vulneraciones de las normas de tratamiento de la información y de los activos de información relevantes de VIATEP IBERICA, que deberán ser debidamente investigados por personal con la experiencia y cualificación adecuadas.

Cada usuario del sistema de información está obligado a reportar inmediatamente una violación (o sospecha razonable) de la seguridad de la información a través del ejecutivo pertinente al Gerente de Seguridad de la Información, quien es responsable de su registro y coordinación de investigaciones en el caso de cooperación con las autoridades policiales. .

La investigación de incidentes de seguridad es realizada por el Gerente de Seguridad y el Equipo de Seguridad. Los incidentes de seguridad se registran y las amenazas y los riesgos relacionados se evalúan periódicamente. El resultado es una mejora en la prevención de la ocurrencia de incidentes de seguridad y por ende la mejora de todo el sistema de seguridad de la información

7.10 Řízení kontinuity činnosti organizace/ Gestión de la continuidad de las actividades de la organización

VIATEP IBERICA zajišťuje připravenost informačního systému na zvládání krizových situací a na zachování svých základních funkcí. Rozsah a formu upřesňuje v Plánu kontinuity informačního systému VIATEP IBERICA.

Požadavky na Plán kontinuity stanovuje Manažer bezpečnosti a bezpečnostní tým na základě hodnocení rizik. Přechod na krizové řízení informačního systému má v kompetenci Manažer bezpečnosti informací, který je též odpovědný za přijetí preventivních opatření.

VIATEP IBERICA asegura la disponibilidad del sistema de información para gestionar situaciones de crisis y mantener sus funciones básicas. El alcance y forma se especifica en el Plan de Continuidad del Sistema de Información de VIATEP IBERICA.

Los requisitos para el Plan de Continuidad son determinados por el Gerente de Seguridad y el equipo de seguridad en base a una evaluación de riesgos. La transición a la gestión de crisis del sistema de información es responsabilidad del Gerente de Seguridad de la Información, quien también es responsable de tomar medidas preventivas.

7.11 Soulad s požadavky/ Cumplimiento de requisitos

VIATEP IBERICA se zavazuje dodržovat soulad se všemi relevantními zákonnými a smluvními požadavky včetně autorských práv a licenčních podmínek dodavatelů programového vybavení. VIATEP IBERICA rovněž přijímá a provádí opatření k zajištění ochrany osobních údajů a citlivých údajů v souladu se zákony a jinými právními předpisy.

V VIATEP IBERICA je prováděno posouzení shody dokumentu Bezpečnosti politika VIATEP IBERICA a navazujících předpisů se skutečným stavem bezpečnosti informací a zajištění souladu informačního systému VIATEP IBERICA s příslušnými technickými zásadami interními audity. Vedoucí pracovníci jednotlivých organizačních jednotek skupiny firem VIATEP IBERICA přijímají a provádějí opatření k zajištění bezpečnosti informací dle místních podmínek na základě metodického řízení Manažera bezpečnosti informací.

VIATEP IBERICA se compromete a cumplir con todos los requisitos legales y contractuales pertinentes, incluidos los derechos de autor y los términos de licencia de los proveedores de software. VIATEP IBERICA también adopta e implementa medidas para garantizar la protección de datos personales y datos sensibles de conformidad con las leyes y demás disposiciones legales.

VIATEP IBERICA evalúa la conformidad del documento de Política de Seguridad de VIATEP IBERICA y la normativa posterior con el estado actual de la seguridad de la información y asegura el cumplimiento del sistema de información de VIATEP IBERICA con los principios técnicos pertinentes mediante auditorías internas. Los gerentes de las unidades organizativas individuales del grupo de empresas VIATEP IBERICA adoptan e implementan medidas para garantizar la seguridad de la información de acuerdo con las condiciones locales basadas en la gestión metódica del Gerente de Seguridad de la Información

7.12 Odkazy na dokumentaci / Enlaces a la documentación

Základním dokumentem VIATEP IBERICA je příručka Integrovaného systému managementu, kde jsou popsány jednotlivé procesy a jejich vzájemná součinnost, včetně odkazů na řídící systémovou dokumentaci VIATEP IBERICA.

El documento base de VIATEP IBERICA es el manual del Sistema Integrado de Gestión, donde se describen los procesos individuales y su mutua cooperación, incluyendo enlaces a la documentación del sistema de gestión de VIATEP IBERICA.

7.13 Pojmy/ Conceptos

akceptace rizika	rozhodnuti přijmout riziko
aktivum	cokoliv, co má pro organizaci hodnotu
analýza rizik	systematické používání informací k odhadu míry rizika a k určení jeho zdrojů
vyhodnocení rizik	proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu
zbytkové riziko	riziko, které zůstává po ošetření rizik
zvládání rizik	proces výběru a přijímání řídících opatření pro modifikaci rizika
bezpečnost informací	ochrana důvěrnosti, integrity a dostupnosti informací
dostupnost	zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby
důvěrnost	zajištění, že informace jsou přístupné pouze těm, kteří jsou k přístupu oprávněni

integrita	zajištění správnosti a úplnosti informací a metod jejich zpracování
posuzování rizik	celkový proces analýzy a hodnocení rizik
management rizik	koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika
plán kontinuity (havarijní plán IT)	plán zajištění kontinuity činnosti organizace v případě nepředvídané události, kdy jsou některé podpůrné procesy, včetně systémů IT poškozeny nebo jsou nedostupné
incident v rámci systému managementu bezpečnosti informací	jednotlivá událost nebo řada nechtěných nebo neočekávaných událostí souvisejících s bezpečností informací, s významnou pravděpodobností, že by mohly poškodit funkce organizace a ohrozit bezpečnost informací
informační systém (IS)	funkční celek, nebo jeho část, zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.
plán obnovy	plány obnovy po nepředvídatelné události popisují, jak obnovit činnost systémů IT, ovlivněných nežádoucím incidentem
prohlášení o aplikovatelnosti	dokument popisující cíle kontrol a nástroje řízení, které jsou relevantní a aplikovatelné na ISMS organizace, a které jsou založeny na výsledcích a závěrech procesů hodnocení a zvládání rizik
systém řízení bezpečnosti informací (Information Security Management System)	Information Security Management System (Systém managementu bezpečnosti informací) (Systém řízení bezpečnosti informací – SŘBI) (Systém řízení informační bezpečnosti – SŘIB) Část celkového systému managementu organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na vybudování, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšováni bezpečnosti informací POZNÁMKA Systém managementu zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje.
událost v rámci systému managementu bezpečnosti informací	identifikovaný výskyt stavu, indikujícího možné narušení nebo chybu zabezpečení, nebo předem neznámá situace, které mohou mít vliv na bezpečnost informací v rámci systému, služby nebo sítě

aceptación del riesgo	decidir aceptar el riesgo
Activo	cualquier cosa de valor para la organización
análisis de riesgo	uso sistemático de la información para estimar el nivel de riesgo y determinar sus fuentes
Evaluación de riesgos	el proceso de comparar un riesgo estimado contra criterios dados para determinar su importancia
riesgo residual	el riesgo que permanece después del tratamiento del riesgo

gestión de riesgos	el proceso de selección y adopción de medidas de gestión para la modificación del riesgo
seguridad de información	protección de la confidencialidad, integridad y disponibilidad de la información
disponibilidad	asegurar que la información sea accesible a los usuarios autorizados en el momento de necesidad
intimidad	garantizar que la información sea accesible solo para aquellos autorizados a acceder a ella
integridad	Garantizar la corrección y la integridad de la información y los métodos para procesarla.
Evaluación de riesgos	proceso general de análisis y evaluación de riesgos
gestión de riesgos	actividades coordinadas que sirven para gestionar y controlar la organización con respecto a los riesgos
plan de continuidad (plan de emergencia TI)	un plan para asegurar la continuidad de la actividad de la organización en caso de un evento imprevisto cuando algunos procesos de soporte, incluidos los sistemas de TI, están dañados o no están disponibles
un incidente dentro del sistema de gestión de seguridad de la información	un solo evento o una serie de eventos no deseados o inesperados relacionados con la seguridad de la información, con una probabilidad significativa de que puedan dañar las funciones de la organización y amenazar la seguridad de la información
sistema de información (SI)	una unidad funcional, o parte de ella, que garantiza la recopilación, el procesamiento, el almacenamiento y la puesta a disposición de la información de forma deliberada y sistemática. Incluye fuentes de datos e información, portadores, recursos técnicos, de programas y de trabajo, tecnologías y procedimientos, estándares relacionados y personal.
plan de recuperación	los planes de recuperación ante desastres describen cómo restaurar el funcionamiento de los sistemas de TI afectados por un incidente adverso
declaración de aplicabilidad	un documento que describe los objetivos de control y las herramientas de gestión que son relevantes y aplicables al SGSI de la organización, y que se basan en los resultados y conclusiones de los procesos de evaluación y gestión de riesgos
sistema de gestión de seguridad de la información (Sistema de Gestión de Seguridad de la Información)	Sistema de gestión de seguridad de la información (Sistema de Gestión de Seguridad de la Información) (Sistema de gestión de seguridad de la información - SŘBI) (Sistema de gestión de seguridad de la información - SŘIB) Parte del sistema de gestión general de la organización, basado en el enfoque (de la organización) de los riesgos de las actividades, que tiene como objetivo construir, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. NOTA Un sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

un evento dentro del sistema de gestión de seguridad de la información	la ocurrencia identificada de una condición que indica una posible brecha de seguridad o vulnerabilidad, o situaciones previamente desconocidas que pueden afectar la seguridad de la información dentro de un sistema, servicio o red

7.14 Použité zkratky/ Abreviaturas

IS	Informační systém
ICT	informační a komunikační technologie
ISMS	Information Security Management System Systém řízení bezpečnosti informací popř. Systém managementu bezpečnosti informací
ISŘ	Integrovaný systém řízení kvality, ochrany ŽP a bezpečnosti informací
IT	Informační technologie
PDCA	model PDCA (Plan-Do-Check-Act) - procesní přístup prosazovaný normou ISO/IEC 27001 pro ustavení, zavedení, provozování, monitorování a zlepšování efektivnosti ISMS v organizaci.

SI	Sistema de informacion
TIC	tecnologías de la información y la comunicación
SGSI	Sistema de gestión de seguridad de la información Sistema de gestión de seguridad de la información o sistema de gestión de seguridad de la información
SICC	Un sistema integrado de control de calidad, protección ambiental y seguridad de la información
TI	Tecnologías de la información
PDCA	el modelo PDCA (Plan-Do-Check-Act) - un enfoque de proceso promovido por el estándar ISO/IEC 27001 para establecer, implementar, operar, monitorear y mejorar la efectividad del SGSI en la organización.

Typ dokumentace: Tipo de documento:	Veřejný dokument Documento público
Verze: Versión	01
Autor(jméno, datum, podpis): Autor:	Gema Carnerero Romero
Schválil (jméno, datum podpis): Aprovado por:	David Hanzlik
Platnost od: Válido desde:	01/08/2022
Revize:	18/08/2022

Revision:	