

**Information Protection Questionnaire**

for Third Party Service Providers

*Questionário de Segurança para Parceiros e Fornecedores*

**Purpose**: This questionnaire has been designed to help assess the information protection practices of third party service providers. The responses provided will help Personal Finance assess the alignment of service providers with industry security practices, as well as to determine the level of compatibility with Personal Finance’s own internal information protection and privacy requirements.

***Objetivo:*** *Este questionário foi projetado para ajudar a avaliar as práticas de proteção de informação de parceiros e fornecedores. As respostas visam ajudar o Personal Finance a avaliar o alinhamento dos prestadores de serviços com os standards de segurança da indústria, bem como determinar o grau de conformidade com os requisitos de privacidade e proteção de informação em vigor no Personal Finance.*

**Instructions:** For each question below, indicate whether or not you meet the information protection objective by responding with a Yes, No, Partial, or N/A in the space provided. For each question, you must also provide additional comments or details to explain the response provided. Note that a critical focus of this assessment is on assuring that sustaining processes have been in place for a minimum of six months. If a particular objective has not been consistently met for a minimum of six months, please respond with “Partial” or “No” as appropriate, and then provide additional details about your level of compliance in the Comments / Details space provided.

***Instruções:*** *Para cada uma das questões abaixo, indique se cumpre ou não os objetivos de segurança de informação respondendo com “Sim”, “Não”, “Parcialmente” ou “N/A”. Para cada questão, deverá fornecer comentários ou detalhes adicionais para complementar a resposta dada. O objetivo desta avaliação é assegurar que os processos de sustentação tenham sido implementados pelo menos durante seis meses. Se um determinado objetivo não tiver sido cumprido por um período consistente e contínuo de seis meses, responda com “Não” ou “Parcialmente”, conforme apropriado e forneça detalhes adicionais no campo de comentários.*

|  |  |
| --- | --- |
| **Company Name / *Empresa*** | SIBS FPS |
| **First Name / *Nome*** |  |
| **Last Name / *Apelido*** |  |
| **Job Title / *Função*** |  |
| **Email** |  |
| **Business Phone / *Telefone*** | 217 813 000 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 1 | Do you conduct or arrange in-house vulnerability scanning for all infrastructure, servers, databases and applications, on at least a quarterly basis? Please describe how vulnerability scanning reports are used by your company and how remediation of vulnerabilities occurs. | Yes | Scans are conducted quarterly. The identified vulnerabilities are analyzed and reclassified based on the CVSSv3 calculator. When vulnerabilities are identified, they are reported to the respective departments with a maximum resolution date considering its severity. After its resolution re-scans are conducted to verify if they were correctly resolved. | *Realiza testes internos de vulnerabilidade a toda a infraestrutura, servidores, bases de dados e aplicações com uma periodicidade pelo menos trimestral? Por favor descreva como são os relatórios usados pela sua empresa e como se processa a correção de vulnerabilidades.* |
| 2 | Does your computing environment undergo external penetration testing by an independent, qualified vendor at least once per year? Please describe how penetration testing reports are used by your company and how remediation of vulnerabilities occurs. | Yes | Penetration Testing is performed annually by both internal and external entities.  For each vulnerability, a plan is defined for its resolution and a corresponding implementation date considering the severity. After solving the vulnerabilities, tests are conducted to verify if they were correctly resolved. | *Realiza testes externos de penetração por um parceiro independente, pelo menos uma vez por ano? Por favor descreva como são os relatórios usados pela sua empresa e como se processa a correção de vulnerabilidades.* |
| 3 | Can Personal Finance perform coordinated / scheduled site audits of the hosting facility? | Parcial | SIBS as several audits to the hosting facilities.  Due to the number of clients, requests must be analysed case by case. | *Autoriza o Personal Finance a realizar auditorias (coordenadas/agendadas) ao seu Datacenter?* |
| 4 | Can Personal Finance perform coordinated / scheduled penetration testing of the hosting facility and/or relevant applications? | No | Due to PCI DSS, SIBS perform internal and external annual penetration. A qualified external company performs the tests. | *Autoriza o Personal Finance a realizar testes de penetração (coordenados/agendados) ao seu Datacenter ou aplicações relevantes?* |
| 5 | Does your organization undergo an external audit examination (SSAE 16 or equivalent) at least annually? If yes, please provide report to Personal Finance. | No | SIBS is under an annual financial audit by Bank of Portugal that includes technical controls.  Is PCI DSS certified and the assessments are performed, on site, annually. | *A sua organização é avaliada por uma auditoria externa (SSAE 16 ou equivalente) pelo menos anualmente? Em caso afirmativo, por favor forneça o relatório ao Personal Finance.* |
| 6 | Is all computing equipment located in a physically secure facility, where electronic access controls are used to prevent unauthorized access to computing facilities? Please describe what physical security controls are available (e.g., access cards, caged equipment rooms, biometrically controlled vaults, etc.) and whether such controls are included in your basic service price. | Yes | Yes, SIBS has human surveillance 24/7, CCTV, access control with multifactor authentication (card access and biometric), SAS (security Airlock System), GTT (Goods & Tools Trap), anti-pass back system, intrusion detection, etc.  These control systems are implicit and therefor constitute the basic service and are not optional. | *Os servidores estão localizados numa instalação fisicamente segura com controlo de acesso eletrónico por forma a evitar acessos não autorizados? Por favor descreva os controlos de segurança física disponíveis (cartões de acesso, jaulas, controlo biométrico…) e se esses controlos estão incluídos no preço do serviço básico.* |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 7 | Are firewalls configured based on the principle of least privilege, where firewalls only allow approved applications, protocols, and services required to meet business needs? Please describe the network connectivity (protocols and ports) needed between Personal Finance and the hosting provider, including client access, integrations with Personal Finance systems, and any data transfers required for your solution to function properly. | Yes | Firewalls are configured based on the principle of least privilege and only applications, protocols, and services required to meet business needs are allowed.  If necessary, a quick on site meeting can be schedule in order to present the network connectivity. | *As firewalls estão configuradas com o princípio do privilégio mínimo, onde estão apenas permissionados os protocolos e serviços necessários para responder às necessidades de negócio? Descreva a conetividade de rede (protocolos e portas) necessária entre o Personal Finance e o Datacenter, incluindo o acesso do cliente, integrações com o Personal Finance e quaisquer mecanismos de transferência de dados para que a solução funcione corretamente.* |
| 8A | Are intrusion detection or intrusion prevention systems used to monitor and/or protect your network? Please indicate whether intrusion detection/prevention is included in your basic service price or whether it is provided as an additional cost. | Yes | Intrusion detection systems are used to monitor and/or protect the network on perimeter interfaces and on all critical internal segments.  Not to have intrusion detection and prevention systems is not an option. | *Utiliza sistemas de deteção ou prevenção de intrusão na sua rede? Indique se a deteção/prevenção de intrusão está incluída no preço de serviço básico ou se é fornecida com um custo adicional.* |
| 8B | Are intrusion detection/prevention systems configured to block suspicious traffic, rather than to report only? | Yes | The IDS does not block the traffic given the impacts that IPS false positives generate. We complement the IDS with Firewalls, WAFs, and other controls that block the suspicious traffic and our SOC team handles these alerts. | *Os sistemas de deteção/prevenção de intrusão estão configurados para bloquear ativamente tráfego suspeito ou apenas realizam log do mesmo?* |
| 9 | Is encryption used to protect the confidentiality of transmitted information, especially for personal information and confidential business information? Examples might include SSL, SSH, SFTP or IPSec. Please describe your capabilities. | Yes | SIBS protects critical data when stored and in transit. When in transit, SIBS uses security standard communication protocols such as TLS, IPSEC, HTTPS, FTPS, SSH, etc.  When the level of risk is higher, the data benefits from an additional protection based on its integrity, authenticity and confidentiality with applicational cryptography such as 3DES, AES, HMAC, PBKDF2, etc. | *Utiliza encriptação para proteger a confidencialidade das informações transmitidas, em particular para informações pessoais ou comerciais confidenciais? Os exemplos podem incluir SSL, SSH, SFTP ou IPSec. Por favor descreva.* |
| 10 | Is encryption used to protect the confidentiality of stored information, especially for personal information and confidential business information? Examples might include database encryption, PGP, or XML Encryption. Please describe your capabilities. | Yes | Data is protected according to its level of criticality. All confidential data is ciphered. Critical cryptographic keys are stored in FIPS 140 compliant HSMs. The principle of least privilege is applied to every production system/application. | *Utiliza encriptação para proteger a confidencialidade das informações armazenadas, em particular para informações pessoais ou comerciais confidenciais? Os exemplos podem incluir encriptação de dados nas BD’s, PGP ou XML Encryption. Por favor descreva.* |
|  | **Information Protection Objective** | **Yes (Sim) / No (Não) / Partial (Parcialmente) / NA** | **Comments / Comentários** | **Objetivo de Segurança de Informação** |
| 11 | Do you encrypt data backups? If yes, please describe what technology is used, what information is contained on the encrypted backup media, and what, if any, information is contained on backup media that is not encrypted. If yes, please indicate whether this is included in your basic service price or whether there is an additional cost for this capability. | Yes | Data is encripted using the Eternus platform (AES256). | *Utiliza encriptação nos seus backups? Em caso afirmativo, descreva a tecnologia utilizada e quais os backups que são encriptados e não encriptados. Indique se este serviço está incluído no preço do serviço básico ou se tem um custo adicional.* |
| 12 | Are encryption keys managed according to security best practices, including policies for who has access to decrypt, protection of private keys, and periodic key rotation? Please briefly describe your key management practices. | Yes | Cryptographic keys are stored in FIPS 140 compliant HSMs. We have a Cryptographic Management requirements are defined in a dedicated Security Policy document. This document defines the Cryptographic infrastructure (HSM, Security Officers and Key Custodians) and Key life cycle (Pre-operational ceremonies and registry; Operational storage, usage, transport, substitution, backup, recovery and revocation; and Post-operational archive and destruction). | *As chaves de encriptação são geridas de acordo com as melhores práticas de segurança, incluído a existência de política de acesso, proteção de chaves privadas e rotação de chaves periódicas? Descreva sucintamente as suas principais práticas de gestão.* |
| 13 | Do you require your employees and contractors to use strong authentication (more than just a password, such as two factor authentication) for remote access to all systems that would store or process Personal Finance data? If yes, please indicate what strong authentication mechanisms are used. | Yes | Yes, we require 2FA for remote access. Depending on the system level of criticality we use: CAP (card and OTP) or password and SMS swivel OTP. | *Exige aos seus colaboradores (internos e externos) que utilizem mecanismos de strong authentication (mais do que uma password, como autenticação de dois fatores) para acesso remoto a todos os sistemas que armazenariam ou processariam dados do Personal Finance? Em caso afirmativo indique quais os mecanismos de strong authentication utilizados.* |
| 14 | Within your own corporate network, do you have standards for strong password composition, periodic changes, and a minimum of 8 characters for all computer accounts used by your system administrators, employees, and/or contractors? Please describe your password standards for both regular user accounts and for administrative accounts. | Yes | Our Security Policy for Authentication credentials defines requirements for password selection usage, change that include many requirements such as minimum length, composition, rotation, etc. | *Dentro da sua rede corporativa, possui standards implementados para composição de passwords fortes, mudanças periódicas e com um mínimo de 8 carateres para todas as contas usadas pelos administradores de sistemas (internos e externos)? Descreva os standards usados para contas de utilizador normais e administrativas.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 15 | Do you conduct or require background screenings for all personnel (employees and contractors) that have access to critical infrastructure, servers, applications, or data? Please describe your process. | Yes | Our Security Policy for Personnel defines requirements for the personnel lifecycle including: Recruitment, Selection, Contract, Reception, Activity, Change of Functions and Termination.  All personnel have background screening upon contract and critical staff have periodic background screening. | *Tem algum processo para verificar o background dos colaboradores que trabalham com a infraestrutura crítica (rede, servidores, aplicações ou dados)? Por favor descreva.* |
| 16 | Do you use documented security configuration baselines to harden and secure IT systems? Please describe how you ensure that security baselines are implemented and working effectively. | Yes | Yes, we have documents that define lockdown requirements.  We test the configuration in a Test environment, and only after accomplishing the intended security configuration and documented it, the configurations are replicated to the production environment. Frequent audits guarantee that baselines are implemented effectively. | *Tem algum processo de hardening aos sistemas de TI com bases de dados de configurações de segurança e/ou processos documentados? Descreva como garante que as baselines de Segurança são implementadas e estão a funcionar corretamente.* |
| 17 | Are automated mechanisms used to ensure that operating systems, security configurations, and networks are kept up-to-date and accurate? Please describe any automated mechanisms you have in place. | Partial | All the System infrastructure is isolated from the external connections, including the internet, for security purposes. Therefore, much of the update process is performed manually. | *São utilizados mecanismos automáticos por forma a garantir que os sistemas operativos, configurações de segurança e de rede estão atualizadas e precisas? Por favor descreva os mecanismos que têm em funcionamento.* |
| 18 | Do you have standards for applying security patches with defined implementation schedules? Please describe the implementation schedule you use for deploying patches | Yes | Our Security Policy for Patches and upgrades define the requirements for this process. As an example critical vulnerabilities should be applied within 60 days. | *Possui procedimentos para aplicar patches de segurança com cronogramas de implementação definidos? Descreva o processo utilizado para implementar patches.* |
| 19A | Do you have a documented change management process in place? Please describe your process. | Yes | Yes, we have an ISO 20000 framework that describes the change management process thoroughly. | *Possui algum processo de Change Management? Por favor descreva o mesmo.* |
| 19B | Do you use automated systems to track changes made to large, complex information systems? Please describe any management systems that are in place. | Yes | We use discovery mechanisms for this process although they are limited to some systems given that they pose a risk resulting from opening discovery routes in our infrastructure. | *Possui algum sistema automático para detetar alterações efetuadas em sistemas de alta complexidade? Descreva todos os sistemas de gestão existentes.* |
| 20 | Do you maintain security precautions that are similar to or consistent with industry best practices, as documented in standards such as ISO/IEC 27002? Please indicate what industry practices or certifications you align with. | Yes | ISO 27002, ISO 20000, PCI-DSS, PCI-PIN, etc. | *Mantém precauções de segurança semelhantes ou consistentes com as best practices da indústria como documentado na ISSO/IEC 27002?*  *Indique as práticas e certificações com as quais está alinhado.* |
|  | **Information Protection Objective** | **Yes (Sim) / No (Não) / Partial (Parcialmente) / NA** | **Comments / Comentários** | **Objetivo de Segurança de Informação** |
| 21 | Do you provide a segregated environment (physically or logically) so that each customer’s data is isolated and protected against any unauthorized access? Please describe. | Yes | Yes, wherever adequate.  Physical segregation is not applied (ex. seperate firwalls, routers, servers, database servers, etc) however, Logical segregation is applied mainly through access control systems. | *Disponibiliza ambientes segregados (física ou logicamente) para que os dados de cada cliente sejam isolados e protegidos de acessos não autorizados? Por favor descreva.* |
| 22 | If hosting multiple customers’ data on one server, are backup tapes maintained such that each customer’s data is kept logically separate from other customer’s data when it is backed up? If yes, please indicate whether this is included in your basic service price or whether there is an additional cost for this capability. | No |  | *Caso aloje dados de vários clientes num mesmo servidor, as tapes de backup são geridas por forma a que os dados de cada cliente sejam mantidos logicamente separados dos dados dos restantes clientes aquando do processo de backup? Em caso afirmativo, indique se esta funcionalidade está incluída no preço do serviço básico ou se tem algum custo adicional.* |
| 23 | Do you have a documented process to securely transport personal or confidential information on physical media such as flash memory, computer hard drives, removable disks, tapes or other media? Please describe your process. | Yes | Yes, the requirements are defined in our Security Policy for Data Classification (PSI-Classificação de Informação\_v04.03). | *Possui um processo documentado para o transporte seguro de informações pessoais ou confidenciais em dispositivos físicos como pens USB, discos rígidos de computadores, tapes ou outros? Descreva o processo.* |
| 24 | Do you maintain detailed audit logs that capture at a minimum a) host name, b) account identifier, c) date and time stamp, d) activity performed, and e) source network address? Please indicate whether audit logging is enabled by default. | Yes | Yes, the requirements are defined in our Security Policy for Audit logs and inspections. Audit logs are enabled by default and we have a high level of auditing activated. | *Mantém registos de auditoria detalhados que permitem identificar, no mínimo: a) hostname b) nome da conta c) data e hora d) atividade executada e) IP de origem? Indique se o audit log está ativado por defeito.* |
| 25 | Do you follow a process to regularly review audit logs for abnormal system events, potential system compromise, etc.? Please describe your process. | Yes | Yes, our SOC team monitors and reviews the audit logs through our centralized SIEM system that correlates security events. | *Possui um processo de revisão de logs para eventos anómalos, intrusão, etc? Descreva o seu processo.* |
| 26 | Are audit logs protected from unauthorized access, modification, and accidental or deliberate destruction? Please describe how audit logs are protected. | Yes | The integrity of the logs is guaranteed through the centralization of all audit trail files on the SIEM. Some critical logs have further mechanisms such as MACs, FIMs etc. | *Os logs de auditoria estão protegidos contra acesso não autorizado, modificação e destruição acidental ou deliberada? Por favor descreva os mecanismos de proteção implementados.* |
| 27 | Do you back up and retain audit logs for a minimum of 90 days? If no, please indicate your standard retention period. | Yes | Yes. | *Efetua backup e retém os logs no mínimo durante 90 dias? Caso contrário indique o seu período de retenção standard.* |
|  | **Information Protection Objective** | **Yes (Sim) / No (Não) / Partial (Parcialmente) / NA** | **Comments / Comentários** | **Objetivo de Segurança de Informação** |
| 28 | Do you have a security incident response process in place, with personnel available on a 24x7 basis to respond to information protection incident alerts? Please describe the capabilities of your incident response process. | Yes | We have security policy that describes our security incident response process (Manula de Procedimentos Plano de Resposta a Incidentes de Segurança de Informação). We have a SOC team available on a 8x5 basis. The SOC team analyzes and monitors all the traffic and events that are aggregated in the SIEM. Inside SIEM we create specific channels with the most important types of events and correlations that if triggered, require additional investigation. There also a daily investigation on the IDS events.  Furthermore we have a 24x7 fraud detection team, 24x7 operations team. | *Possui algum processo de resposta a incidentes de segurança com recursos disponíveis 24x7 para responder a alertas de incidentes de proteção de informação? Descreva o seu processo de resposta a incidentes.* |
| 29 | Are you able to notify Personal Finance of an information protection incident within one hour of becoming aware of the incident? If not, what time period can you commit to? | Yes | We will align with regulation on this matter. Our first priority will be to contain the attack and protect our customers data. We will inform any involved party as quickly as possible. | *Consegue notificar o Personal Finance acerca de um incidente relacionado a segurança de dados dentro de uma hora após ter tomado conhecimento do incidente? Caso contrário, qual o período com que se consegue comprometer?* |
| 30 | If an information protection incident was to occur, are you able to provide audit logs to Personal Finance for our review? | Yes | Yes, we will collaborate in any investigation. | *Em caso de incidente, consegue disponibilizar logs ao Personal Finance para que possamos rever o incidente?* |
| 31A | Do you have a documented business continuity or disaster recovery plan that covers the specific services that Personal Finance is requesting (e.g. infrastructure, applications, IT support, etc.)? | Yes | Yes. | *Possui um plano de Disaster Recovery ou de Business Continuity que cubra os serviços específicos que o Personal Finance está a solicitar (infraestrutura, aplicações, suporte de TI…)?* |
| 31B | Has your business continuity or disaster recovery plan been reviewed for applicable updates within the last 12 months? | Yes | Yes! minor revisions are made after every annual disaster recovery exercise. Additionally there is an ongoing major revision that is expected to be completed in Q1/2018. | *O seu plano de Disaster Recovery ou de Business Continuity foi revisto nos últimos 12 meses?* |
| 31C | Has your business continuity or disaster recovery plan been tested within the last 12 months? Please describe the level of disaster recovery testing that was most recently performed (e.g. tabletop testing, failover in test environment, full production failover, etc.) | Yes | The BCP is tested once a year in all environments (Certification/Quality/Production) and always a full failover level. | *O seu plano de Disaster Recovery ou de Business Continuity foi testado nos últimos 12 meses?*  *Por favor descreva o último teste de Disaster Recovery.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 32 | Do you minimize single points of failure in your computing environment by implementing controls such as component redundancy, real-time monitoring or backup, transaction recovery, replacement equipment, high availability hardware, or redundant power sources? Please explain, and indicate whether such items are included in your basic service price or whether there is an additional cost for these items. | Yes | [DSI] By default we make use of component redundancy, real-time monitoring, backup, transaction recovery, replacement equipment, high availability hardware and redundant power sources.  These features are by default and are not an option. | *Minimiza a existência de single points of failure no seu ambiente implementando controlos como componentes redundantes, monitorização em tempo real, backup, recuperação de transações, equipamentos de substituição, hardware de alta disponibilidade ou fontes de energia redundantes? Explique e indique se estes itens estão incluídos no preço do serviço básico ou se têm custo adicional.* |
| 33 | Do you handle any credit card information as part of your service offerings? If yes, please provide your latest certificate or attestation of PCI compliance. | Yes | The latest certificates can be found at the Visa site or Mastercard relevant sites. SIBS is identified as SIBS FPS. | *Gere ou administra informações de cartões de crédito como parte das suas ofertas de serviços? Em caso afirmativo, forneça o seu certificado mais recente de conformidade PCI.* |
| 34 | Application Development - If your organization developed an application that Personal Finance will be using (such as a SaaS or hosted model): | Yes |  | *Desenvolvimento de Aplicações: se a sua organização desenvolveu alguma aplicação que o Personal Finance usará (como modelo SaaS ou hosted):* |
| 34A | If your organization developed an application that Personal Finance will be using, is security a core component within your design and development process? Please describe. | Yes | Yes. Security is incorporated in the very beginning of product development. The first Product document is the Business Requirements document and this template includes a section for Security Requirements. | *Se a sua organização desenvolveu uma aplicação que o Personal Finance irá usar, a segurança é um componente central no seu processo de design e desenvolvimento? Por favor descreva.* |
| 34B | Is your organization’s application development process based on an industry best practices framework that ensures that security is included throughout the entire software development life cycle (SDLC) process? Please describe. | Yes | SIBS is certified ISO 20000.  Developers are trained annually in up-to-date secure coding techniques.  Secure coding guidelines are defined.  SIBS perform automatic code revision. | *O processo de desenvolvimento de aplicações da sua organização é baseado numa estrutura de best practices da indústria que garanta que a segurança esteja incluída ao longo de todo o ciclo de vida do desenvolvimento de software (SDLC)? Por favor descreva.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 34C | Do you proactively protect against common application attacks, such as input tampering, injection flaws (such as SQL Injection), replay attacks, Cross Site Scripting, manipulation of application logic, and privilege escalation? Please describe your development practices that are used to ensure security of the application. | Yes | Source Code is analysed to find any security vulnerabilities. | *Protege-se proactivamente contra ataques comuns de aplicações como input tampering, injection flows (como SQL injection), replay attacks, Cross Site Scripting, manipulação de lógica de aplicações e escalonamento de privilégios? Descreva as práticas de desenvolvimento usadas para garantir a segurança da aplicação.* |
| 34D | Does your organization have strict controls in place to restrict access to program source code and related libraries? | Yes | Yes | *A sua organização possui controlos rigorosos para restringir o acesso ao código-fonte do programa e bibliotecas relacionadas?* |
| 35 | Application Security Testing - If your organization developed an application that Personal Finance will be using (such as a SaaS or hosted model): | -- | -- | *Testes de Segurança a Aplicações – se a sua organização desenvolveu uma aplicação que o Personal Finance irá utilizar (como modelo SaaS ou hosted):* |
| 35A | Does your application undergo security penetration testing on a regular basis? If yes, please indicate the frequency, and whether this is performed by an independent vendor, by in-house resources, or both. | Yes | There are both Internal and external Penetration testing in a yearly basis and at every major change. | *A sua aplicação é submetida a testes de penetração de segurança de forma regular? Em caso afirmativo indique a frequência dos testes e se são realizados por entidades externas, equipas internas, ou ambos.* |
| 35B | Do you perform code reviews that specifically address security issues in code? If yes, please describe whether these code reviews are performed by peers within your organization, or by an independent company, or both. |  | Yes. They are performed by the Security Department. | *A sua aplicação é submetida a code review com vista a identificar problemas de segurança no código? Em caso afirmativo indique a frequência dos testes e se são realizados por entidades externas, equipas internas, ou ambos.* |
| 36 | For user password authentication within your application/solution: |  |  | *Para autenticação de utilizadores na sua aplicação/solução:* |
| 36A | Do you always use encryption or one-way hash algorithms to protect stored passwords? | Yes | Yes | *Utiliza algoritmos de encriptação para proteger passwords armazenadas de forma permanente?* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 36B | Are you capable of locking accounts after a set number of incorrect login attempts, where the value is configurable by Personal Finance? | No | No, usually this is a system configuration and not available to be configured by clients. | *Consegue definir o bloqueio automático de contas após um número definido de tentativas incorretas, sendo este valor parametrizável pelo Personal Finance?* |
| 36C | Are you capable of enforcing password complexity, length, and periodic change requirements, where these settings are configurable by Personal Finance? | No | No, usually this is a system configuration and not available to be configured by clients. | *Consegue impor a utilização de passwords complexas, comprimento e requisitos de alteração periódicas, sendo estes valores parametrizáveis pelo Personal Finance?* |
| 36D | Do you have APIs or other mechanisms to support automated provisioning and de-provisioning? | No |  | *Possui API’s ou outros mecanismos para suportar o aprovisionamento e cancelamento automático de contas?* |
| 37 | Do you support any of the following mechanisms for single sign-on authentication, which would allow Personal Finance to leverage our own identity management infrastructure to authenticate users to your application? | N/A |  | *Suporta algum dos seguintes mecanismos de autenticação Single Sign-on que permita ao Personal Finance usar a sua própria infraestrutura para gerir e autenticar utilizadores nas vossas aplicações?* |
| 37A | Security Assertion Markup Language (SAML) 2.0. If no, is SAML 2.0 on your roadmap? | N/A |  | *Security Assertion Markup Language (SAML) 2.0. Caso não possua, está prevista a sua implementação?* |
| 37B | Web Services, using a SOAP interface? | N/A |  | *Web Services com interface SOAP?* |
| 37C | LDAP, using a LAN-to-LAN VPN between your network and Personal Finance? | No |  | *LDAP, usando uma VPN entre a sua rede e o Personal Finance?* |
| 37D | Any proprietary or custom single sign-on solutions? Please describe any custom capabilities you have for integrating with your customer’s existing identity management solutions. | No |  | *Alguma solução de SSO proprietária ou customizada? Por favor descreva as possibilidades de integração com as soluções existentes no cliente.* |
| 38 | Does the application implement a configurable inactivity timeout, where user sessions are invalidated after a period of inactivity? | Yes |  | *A implementação implementa algum tempo limite de inatividade configurável, a partir do qual as sessões de utilizadores são terminadas?* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 39 | Does the application implement levels of access privileges or roles, so that users can be assigned only the permissions they need to perform their respective functions? Please describe. | Yes | We use typically use RBAC. | *A aplicação implementa níveis de privilégio ou de acesso, por forma a que a cada utilizador possam ser atribuídas apenas as permissões necessárias para executar as suas funções? Por favor detalhe.* |
| 40 | Do you proactively address database security concerns, with capabilities such as database hardening guides and procedures, database vulnerability scanning, SQL monitoring, log monitoring, and hiring internal expertise? Please describe. | Yes | Yes, we address database security concerns, taking into account: database hardening guides and procedures, database vulnerability scanning, SQL monitoring and log monitoring. | *Implementa proactivamente algum tipo de segurança de bases de dados, com enfoque em hardening de BD’s, scan de vulnerabilidades, SQL monitoring, log monitoring ou captação de recursos especializados? Por favor descreva.* |
| 41 | If you maintain any wireless networks in your environment, do you require user or machine authentication to all wireless networks, use a strong passphrase key (where applicable) that is changed at least yearly, and scan for rogue access points on a regular basis? Please describe your processes to ensure security of wireless networks. | Yes | There are very few computers that connect to the wireless network. This is a segregated network that cannot interact to the internet directly. There are some verifications by the audit team to scan for rogue access points. | *Caso possua algum tipo de rede sem fios no seu ambiente, estas requerem autenticação de utilizador ou máquina com uma password forte e alterada regularmente? Efetua scans de vulnerabilidades regularmente? Descreva os seus processos para garantir a segurança destas redes.* |
| 42 | Do you have a documented and published privacy policy that strictly prohibits the sale, rental, transfer, trading, or disclosure of Personal Finance provided personal information to third parties? | Yes | On this subject we directly apply the banking Law that do not allow any of such events, and the Nondisclosure contractual obligation about any information related to our clients. | *Possui alguma política de privacidade documentada e publicada que proíba a venda, aluguer, transferência, negociação ou divulgação de informação do Personal Finance a terceiros?* |
| 43 | Do you have documented information protection policies you can make available for Personal Finance review? | Yes | If necessary, a quick on site meeting can be schedule in order to present and review the policies. | *Possui procedimentos documentados de segurança de informação que possa disponibilizar ao Personal Finance para revisão?* |
| 44 | For your employees that handle confidential or personal information, do you provide them adequate security and privacy training? Please describe. | Yes | Every year, the employees must perform a Security Awareness training module. Depending on their functions, additional trainings related to security are applied. | *Os colaboradores que trabalham com informações confidenciais ou pessoais recebem formação específica em segurança e privacidade? Por favor descreva.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 45 | Do you have a documented process to ensure personal information handled by you is processed and protected in accordance with global information protection laws? Please describe your process. | Yes | The requirements are stated in the Security Principles document (SGSI - Principios Gerais de Segurança).  We are currently adapting our process in accordance with the GDPR. | *Possui algum processo documentado para garantir que as informações pessoais geridas pela sua organização são manipuladas e protegidas de acordo com as leis de proteção de dados? Descreva o seu processo.* |
| 46 | Are you willing to sign a Personal Finance contract addendum that ensures industry standard information protection and privacy practices are followed? | Yes | The contact will obviously have to be reviewed before commitment. | *Está disposto a assinar uma adenda ao contrato do Personal Finance, garantindo que os standards e melhores práticas da indústria relativamente a segurança e proteção de dados são seguidos?* |
| 47A | If you have any reliance on third party services that might have custody of Personal Finance information (including backup media storage facilities), are all third parties contractually required to protect information in their possession? | Yes | All third parties are contractually required to protect information. | *Caso dependa de serviços de terceiros que possam ter contato com informações do Personal Finance (incluindo instalações de armazenamento de backups), todos os terceiros são contratualmente obrigados a proteger as informações em sua posse?* |
| 47B | Is a process in place to regularly monitor third party service providers to ensure compliance with security and privacy standards? | Yes | PCI-DSS compliance of third parties are regularly validated. | *Existe algum processo para auditar regularmente terceiros que sejam prestadores de serviços por forma a garantir a conformidade com os standards de segurança e privacidade?* |
| 48 | Has there been theft, breach of privacy, alteration or damage of web server content, denial of service or any other losses in the prior 12 months? If “yes”, what corrective actions have been taken to prevent future incidents? Please provide evidence of any corrective actions taken. | No |  | *Ocorreu algum roubo, violação de privacidade, alteração ou danos em servidores web, Denial of Service ou quaisquer outros incidentes que tenham resultado em perda de informação nos últimos 12 meses? Em caso afirmativo quais as ações corretivas tomadas para evitar incidentes futuros? Forneça evidências de quaisquer ações corretivas tomadas.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Information Protection Objective | Yes (*Sim*) / No (*Não*) / Partial (*Parcialmente*) / NA | Comments / *Comentários* | *Objetivo de Segurança de Informação* |
| 49 | Is your company Safe Harbor Certified? If “yes”, please advise the date of certification. If your company is not Safe Harbor Certified and you handle personal information on a global basis, please explain how you comply with global data transfer laws. | NA |  | *A sua empresa é Safe Harbor Certified? Em caso afirmativo, indique a data da sua certificação. Caso contrário e se manipula informações pessoais de forma global, explique como cumpre as leis internacionais de transferência de dados.* |
| 50 | Do you have the option of locating some or all data operations in a jurisdiction that has stronger privacy protections than the US, such as Canada, Argentina, Israel, New Zealand, or somewhere in the European Union? | Yes | All data is kept on premises in EU | *Tem a opção de localizar algumas ou todas as suas operações de dados numa jurisdição que tenha políticas de privacidade mais fortes que os EUA, como o Canadá, Argentina, Israel, Nova Zelândia ou algum local na União Europeia?* |