INDICE

OBJETIVO E MÉTODO DE APLICAÇÃO

Este documento é funcional, de acordo com as disposições do Procedimento Organizacional, para a identificação dos requisitos de segurança lógica e física (doravante, Requisitos) para a proteção das informações e sistemas/infraestrutura da TIM (doravante denominados TIM Recursos) e determinar as regras comportamentais de referência a serem incluídas no anexo técnico do contrato / contrato de serviços com os fornecedores (doravante, Terceiro).

Os requisitos de segurança descritos neste documento são os mínimos necessário, dependendo do tipo do contrato, outros requisitos de segurança poderão ser informados.

Os Requisitos expressos neste documento foram agrupados com base nos seguintes possíveis métodos operacionais com os quais o Terceiro, que acessa a TIM Recursos, pode fornecer os serviços a serem fornecidos:

A	Proteção de informação
B	Requisitos Organizacionais e para relatar Eventos de segurança de Terceiros
C	Sistema de informação de terceiros
D	Infraestrutura de rede de terceiros
E	Continuidade de negócios

Também deve ser notado que se o Terceiro realizar o processamento de tipos particulares de informação sujeitos a restrições regulatórias adicionais com respeito àqueles para a proteção de dados pessoais já considerados neste anexo (por exemplo, dados de tráfego, Informações *Sensíveis ao Preço*), os Requisitos expressos neste documento devem ser complementados por medidas de segurança adicionais e específicas.

REQUISITOS PARA TERCEIROS (FORNECEDORES TIM)

As políticas de segurança da TIM devem ser seguidas por terceiro que estejam dentro das dependências da TIM.

A. Proteção da informação

No que diz respeito à TIM, *informação* significa qualquer agregação de dados que tenha um valor e um significado para a TIM, qualquer que seja a forma e as tecnologias usadas para seu processamento e armazenamento. A definição de informação inclui qualquer notícia ou comunicação em forma escrita ou verbal, ou qualquer conjunto de "dados estruturados" processados, comunicados, armazenados (manualmente ou por meios automáticos) e utilizados na execução do trabalho, bem como dados em um arquivo ou código de programa.

1) O terceiro deve garantir que as informações proprietárias da TIM sejam processadas, de acordo com os princípios de "*Need to know*" e "*Least Privilege*", exclusivamente dentro do serviço contratual, evitando a divulgação para / ou na presença de pessoas não autorizadas.
2) O terceiro é obrigado a processar as informações da TIM, seja em TI e/ou em forma de papel, salvaguardando a sua *Confidencialidade, Integridade e Disponibilidade*, bem como em conformidade com as Leis atuais.
3) O terceiro deverá ter completa rastreabilidade de acesso realizados nas informações da TIM, afim de identificar origem, autor, data/hora e informação acessada.

B. Requisitos de relatórios de eventos organizacionais e de segurança

1) O terceiro, afim de assegurar a administração ordinária dos aspectos de segurança indicados no presente documento, bem como a gestão de eventos de segurança decorrentes de situações de emergência e/ou acidentes, devem identificar, internamente, uma estrutura / figura de referência para garantir a segurança do serviço prestado, incluindo:
   - *Pessoa de contato de segurança,* corresponde ao Referente que tem a tarefa de assegurar as relações entre o terceiro e a TIM para a gestão transversal de todos os aspectos de segurança. O contato com a segurança deve ser realizado por telefone e endereço de e-mail, previamente comunicados à TIM e disponíveis para o gerenciamento de eventos de segurança, conforme o nível de contrato.
   - *Pessoa para o gerenciamento de acessos,* corresponde ao Referente que tem a tarefa de garantir, em particular, a gestão dos acessos atribuídas pela TIM ao terceiro para permitir o acesso a Recursos da TIM.
2) O Terceiro, através do seu Representante de Segurança deve informar imediatamente a TIM em caso de danos, roubo ou perda de ativos de TI contendo informações proprietárias da TIM, credenciais de acesso, informações da TIM. Em relação aos casos que envolvem dispositivos de autenticação fortes, o Terceiro deve também prever a revogação do certificado contido no dispositivo.

   A comunicação deve ser enviada por e-mail para a pessoa de contato da TIM, a quem o Terceiro normalmente faz referência na prestação de serviços.
3) O Terceiro é obrigado a notificar a TIM sobre todos os eventos, inclusive os acidentais, e sobre as informações detalhadas relativas, que podem ser consideradas como violações de dados pessoais. Esta comunicação deve ser feita estritamente dentro de 24 horas a partir do conhecimento dos eventos acima mencionados e enviada por e-mail para a pessoa de contato da TIM a quem o Terceiro geralmente se

refere na prestação de serviços. Neste sentido, o Terceiro deve preparar ações internas adequadas para garantir essas obrigações (por exemplo, definindo procedimentos apropriados / instruções de operação) e deve garantir assistência à TIM fornecendo prontamente todas as informações adicionais que possam ser solicitadas pela própria para avaliação e gestão corretas dos casos de potencial violação de dados pessoais.

4) As atividades de gerenciamento e resolução de incidentes devem ser devidamente documentadas e arquivadas, provendo toda linha do tempo do processo de tratamento.

5) Caso seja previsto em cláusulas contratuais a possibilidade de utilização de outras empresas para execução do contrato, o mesmo deve garantir que esta empresa siga os requisitos expressos neste anexo técnico.

C. Sistema de informação de terceiros

Sistemas de Informação de Terceiros são os sistemas, plataformas ou, mais geralmente, as ferramentas tecnológicas físicas e lógicas do Terceiro através do qual a informação / dados da TIM são processados. Para estes sistemas de informação, o Terceiro deve assegurar que:

1) Os sistemas de informação que processam dados pessoais de propriedades da TIM estão localizados dentro do Brasil e esses dados só poderão ser transferidos para paises que garantam adequados niveis de proteção de dados pessoais. (Ex: U.S.A – Privacy Shield e U.E GDPR).

2) Eles são mantidos em instalações protegidas e com acesso controlado.

3) Qualquer software instalado em sistemas de informação deve ser legalmente licenciado.

4) Existe um software antivírus atualizado sempre que houver versões disponíveis.

5) Atualizações no sistema operacional e de aplicação necessárias para corrigir defeitos e prevenir vulnerabilidades alinhadas no mínimo com o padrão OWASP TOP 10 devem ser instaladas imediatamente após a disponibilização dos fabricantes.

6) Devem ser efetuadas reconfigurações apropriadas para a modificação / eliminação das configurações da aplicação e padrões do sistema, como senhas, comunidade SNMP, contas e serviços desnecessários; a resolução de vulnerabilidade de segurança conhecidas de acordo com os padrões de proteção.

7) Devem ser adotados procedimentos de backup adequados que contemplem dados da TIM, em concordância com o gestor do contrato. Estes procedimentos devem ser documentados e conter pelo menos a indicação: da frequência, dos métodos de execução, do arquivamento e da retenção dos backups. Os dados devem ser mantidos apenas pela duração do período contratual, após isso, os mesmos devem ser entregues a TIM e eliminados.

8) No caso de avarias ou incidentes nos seus sistemas de informação, devem ser adotados procedimentos operacionais específicos para a execução das atividades de restauração, que devem incluir tempos de implementação acordados com o gestor do contrato.

9) Para sistemas de informação que processam dados pessoais de propriedade da TIM, procedimentos específicos para extração ou transmissão de dados processados deverão ser realizados de forma segura garantindo que não haja vazamento de informações.

10) Todos os usuários de acesso (incluindo os sistemas técnicos e M2M) devem ser identificados e gerenciados de acordo com procedimentos definidos e documentáveis que permitam fornecer evidências das autorizações emitidas para usuários individuais.

11) Todos os usuários devem receber credenciais de acesso individuais, contendo um UserID e uma senha; os UserIDs de um usuário não devem ser atribuídos novamente a outros usuários, mesmo em momentos

diferentes. Para usuários técnicos, o histórico documentado de liberação / uso deve ser fornecido.

12) Os perfis de autorização definidos, para acesso aos dados do sistema, devem garantir a atribuição aos usuários dos corretos privilégios proporcionais às necessidades mínimas para o desempenho das atividades / serviços contratados com a TIM (*Need to Know e Least Privilege*); esses perfis devem ser identificados e configurados antes do início do processamento para documentar os perfis que podem ser associados para cada usuário ou para classes homogêneas de usuários.

13) Uma verificação periódica é realizada, pelo menos a cada três meses, e documentada em relação à necessidade de manter válidos os perfis definidos e as autorizações concedidas aos usuários (incluindo os privilégios de acesso atribuídos).

14) Fornecer aos usuários a manutenção das credenciais de acesso atribuídas a eles, a fim de garantir o sigilo absoluto e impedir seu compartilhamento.

15) Suspender / cessar prontamente os acessos dos usuários da equipe que não estiverem mais atribuídos ao serviço da TIM ou que não precisem mais acessar os dados da TIM. Além disso, os acessos devem ser suspensos e, eventualmente, cessados:

    - Devido a inatividade, após 2 meses do último uso para acesso a sistemas de informação que não manipulam dados pessoais, ou 1 mês no caso de sistemas de informação que processam dados pessoais, incluindo dados de tráfego telefônico / telemático (de acordo com a atual legislação sobre a proteção de dados pessoais);
    - Após várias tentativas de acesso incorretas;
    - Como resultado de uso ilegal ou daqueles que colocam em risco a segurança dos Recursos da TIM, a critério exclusivo da TIM;
    - Na data de expiração especificada na solicitação de autorização (a menos que seja estendida).
    - Caso o usuário tenha saído do Terceiro ou foi avisado pela TIM para remover.

16) A senha de acesso aos sistemas de informação do Terceiro deve, no mínimo, atender às seguintes características:

    - Composto por pelo menos 8 caracteres (pelo menos 1 caracter numérico; pelo menos 1 caracter alfabético; pelo menos 1 caractere especial; não pode conter 3 ou mais caracteres idênticos consecutivos);
    - Deve ser alterado no primeiro acesso;
    - Deve ser substituído pelo menos a cada três meses (somente para UserIDs nominais atribuídos a um indivíduo) e a nova senha deve diferir das quatro anteriores.

17) Medidas adequadas devem ser implementadas para o rastreamento dos usuários e administradores do sistema de terceiros. Essas medidas devem incluir a geração, coleta e armazenamento de registros de acesso (login e logout) e todas as ações realizadas por esses acessos para os quais a integridade, a não repetibilidade e o não-repúdio devem ser garantidos e o armazenamento deve ser no mínimo de 3 anos.

18) Todo sistema e infraestrutura de atendimento a TIM, devem ser avaliados semestralmente em testes de Invasão e analise de vulnerabilidades, assim como todos os controles e ferramentas de proteção devem ser medido e reportados para a TIM.

D. Infraestrutura de rede de terceiros

A infraestrutura de rede de Terceiros refere-se ao conjunto de equipamentos / plataformas de TIC localizados nos escritórios do Terceiro, dentro do qual os sistemas de TI / Workstations de Terceiros que lidam com informações / dados de propriedade da TIM são atestados.

O Terceiro, que realiza atividades em nome da TIM exclusivamente dentro de sua própria infraestrutura de rede, deve garantir que:

1) A parte da rede na qual os sistemas de informação e Workstations de Terceiros são identificados e autorizados a acessar / processar os recursos da TIM, deve ser mantida isolada de outras redes, pelo menos em um nível lógico.

2) Sistemas de informação e dados relacionados residam em redes (ou partes da rede) protegidas por um ou mais firewalls nos quais a implementação de regras destinadas a combater tentativas de acesso não autorizados é garantida.

3) Existe um sistema para monitorar o acesso à sua parte da LAN na qual as Workstations de Terceiros de seus usuários que trabalham para a TIM são atestadas, a fim de detectar quaisquer anomalias ou ameaças que possam comprometer a segurança dos Recursos da TIM.

4) Se, exclusivamente para fins do serviço / atividade contratado, for necessário interconectar a rede de acesso aos recursos da TIM com a rede pública (Internet), essa interconexão não pode ocorrer diretamente, deve incluir mecanismos de proteção, como exemplo de proxy ou gateway de acesso. Sob nenhuma circunstância os recursos de rede de Terceiros responsáveis pelo acesso / processamento dos Recursos da TIM podem ser exibidos diretamente na Internet.

E. Continuidade de negócios

1) Planos de recuperação para a continuidade dos serviços prestados à Tim devem existir para casos interrupção/incidente.

2) Os planos devem ser testados ao menos semestralmente.