ÍNDICE

1. Objetivo 2

2. Aplicação e Áreas envolvidas 2

3. DEFINIÇÕES E PREMISSAS 2

3.1. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO 2

3.1.1. Código de Conduta 3

3.1.2. Documentação Normativa de Segurança da Informação da Organização 4

4. RESPONSABILIDADE 4

4.1. RESPONSABILIDADES GERAIS DO FORNECEDOR DA ORGANIZAÇÃO 4

4.1.1. Identificação de Desvios / Riscos 4

4.1.2. Comunicação de incidentes de segurança da informação 4

5. DESCRIÇÃO DA POLÍTICA 5

5.1. Gestão de ativos 5

5.2. Controle de acesso físico e lógico 5

5.3. Delimitação de perímetro e proteção de segurança física 6

5.4. Uso aceitável de ativos e recursos 6

5.5. Análise e garantias de segurança em sistemas de informação fornecidos 6

5.6. Recursos Humanos, Interações e Comunicações 6

5.7. Planos de Continuidade, Desastre ou Situação de Emergência 7

5.8. Requisitos Legais e Regulamentares adicionais 7

5.9. Criptografia, Privacidade e Monitoramento 7

5.10. Subcontratação 8

6. Referência a outros documentos 8

1. OBJETIVO

O objetivo desta política de segurança da informação é orientar Fornecedores da Organização (ver DEFINIÇÕES E PREMISSAS) sobre as diretrizes de segurança da informação em vigor, assim como descrever sua participação e responsabilidade no cumprimento das metas e estratégias de excelência estabelecidas pela Organização como fornecedora de produtos e serviços de tecnologia da informação. As instruções e regras aqui descritas devem ser seguidas para garantir, de forma consistente e eficiente, a proteção das informações disponibilizadas pela Organização, assim como o uso apropriado de recursos tecnológicos, ambientes e dependências acessados pelos Fornecedores em razão da prestação de serviços, garantindo a correta custódia e evitando ameaças deliberadas ou acidentais.

2. APLICAÇÃO E ÁREAS ENVOLVIDAS

Fornecedores e parceiros da Organização.

3. DEFINIÇÕES E PREMISSAS

Organização: TIVIT, Takoda e demais empresas do Grupo TIVIT conforme aplicável.

3.1. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Todos os Fornecedores da Organização devem estar comprometidos quanto à observação da política de segurança de informação da Organização, não fornecendo ou apropriando-se indevidamente de recursos de informações, utilizando sistemas e recursos tecnológicos somente de acordo com autorizações e instruções especificadas pela Organização, zelando e preservando ativos. Devem estar, ainda, imbuídos de manter e preservar os princípios básicos de segurança da informação:

- Confidencialidade – O Fornecedor deve contribuir para a manutenção do sigilo e restrição de acesso das informações compartilhadas ou acessadas em razão do exercício de sua função e serviço contratado. Todas as informações compartilhadas ou acessíveis ao Fornecedor da Organização devem ser tradadas como sigilosas e pertencentes à Organização.
- Integridade – O Fornecedor compromete-se com o uso adequado e autorizado de ativos da Organização, inclusive informações. Não é permitida a manipulação ou edição de ativos de informações fora do seu escopo de trabalho ou limitações impostas por procedimentos ou controles de acesso em sistemas de informação.
- Disponibilidade – O Fornecedor preza pela preservação dos ambientes e recursos tecnológicos da Organização de seu fornecimento ou suporte, de forma a favorecer a continuidade e oferta ininterrupta de serviços.

É considerado incidente de segurança da informação envolvendo Fornecedores, qualquer desrespeito aos princípios de segurança da informação e, em especial, a violação de dados: caracterizada pela violação de segurança que leva à destruição acidental ou ilícita, à perda ou à divulgação não autorizada, acesso a dados protegidos transmitidos ou armazenados, e transformação ou processamento não permitidos.

Os incidentes de segurança originados por Fornecedores podem ocasionar investigações que resultam em sanções, punições e responsabilizações legais, assim como cancelamentos de contrato e dever de indenizar.

3.1.1. Código de Conduta

É responsabilidade de todos os colaboradores, Fornecedores e parceiros da Organização, a conduta correta e ética, obedecendo os preceitos de respeito às pessoas e preservação da imagem da Organização e seu compromisso com segurança da informação.

Espera-se dos Fornecedores um comportamento ético e de elevado moral, respeito e a observância às leis vigentes assim como dos regulamentos da Organização, incluindo:

- Exercer o trabalho profissional com responsabilidade, dedicação, honestidade e justiça, buscando sempre a melhor solução;
- Esforçar-se para adquirir continuamente competências técnicas e profissionais, mantendo-se sempre atualizado com os avanços da profissão e especialidades;
- Atuar dentro dos limites de sua competência profissional;
- Guardar sigilo profissional das informações que tiver acesso em razão do exercício de suas atividades contratadas;
- Atender às expectativas de confiança depositadas pela Organização, acessando e utilizando recursos e informações apenas no limite da necessidade para realização de seu trabalho e autorização concedida;
- Pautar sua relação com colegas nos princípios de consideração, respeito e solidariedade, assim como conduzir as atividades profissionais, que envolvam interação ou contribuição em grupo, sem discriminação de qualquer tipo, seja de cor, sexo, nacionalidade, idade, religião, estado civil ou qualquer outra condição humana;
- Honrar compromissos e prazos estabelecidos;
- Não praticar atos deliberados que possam comprometer segurança, privacidade ou que atentem para diminuição ou anulação de controles e proteções de segurança estabelecidos pela Organização.

3.1.2. Documentação Normativa de Segurança da Informação da Organização

Para suportar o Sistema de Gerenciamento de Segurança da Informação da Organização (SGSI), aderente à norma nacional ABNT NBR ISO/IEC 27001 para implementar, monitorar e melhorar os controles e indicadores de eficiência e eficácia do processo que garante a segurança da informação na Organização, diversos documentos, procedimentos e instruções são publicadas e atualizadas constantemente. É responsabilidade do Fornecedor a observância destas normativas, ainda que não explicitamente contidas nesta política, específica. Para isso, o Fornecedor deve buscar, sempre que não encontrar orientação suficiente neste documento, instruções específicas junto à Organização e complementar o entendimento dos requisitos de segurança da informação, quando necessário.

O Fornecedor deve manter-se informado dos requisitos e normas da Organização que regulam sua atuação junto à Organização, assim como das atualizações destas documentações.

4. RESPONSABILIDADE

4.1. RESPONSABILIDADES GERAIS DO FORNECEDOR DA ORGANIZAÇÃO

Todos os Fornecedores devem seguir as orientações gerais de segurança da informação e contribuir para a identificação de ameaças e riscos à operação da Organização.

4.1.1. Identificação de Desvios / Riscos

Todo e qualquer impeditivo da prestação de serviço na forma acordada deverá ser reportado a Organização, para que seu impacto seja analisado e comunicado, internamente, minimizando impactos a reputação e imagem da Organização e/ou sua atuação específica contratada.

4.1.2. Comunicação de incidentes de segurança da informação

Os Fornecedores são parte integrante do fluxo de comunicação de eventos de segurança que possam interferir negativamente em sua atuação contratada ou indicar comportamento anormal de recursos de TI em uso. Tais eventos podem vir a ser classificados como incidentes de segurança da informação pela Organização e tratados adequadamente para garantir a integridade e qualidade da infraestrutura de TI da Organização.

Todo comportamento anormal de serviços de rede e sistemas de informação, percebidos pelo Fornecedor, deve ser reportado para: soc.hotline@tivit.com.

5. DESCRIÇÃO DA POLÍTICA

Os Fornecedores devem seguir as orientações específicas de segurança da informação, quando aplicável.

5.1. Gestão de ativos

- Os Fornecedores devem observar regras para o uso de equipamentos computacionais autorizados pela Organização em ambientes de trabalho, tais como aparelhos celulares, tablets, computadores pessoais e wearables. Todos os equipamentos computacionais trazidos para o ambiente de trabalho, nas dependências da Organização, devem ser declarados.
- O Fornecedor que usar equipamentos computacionais de propriedade da Organização deve utilizá-lo apenas para os fins descritos na contratação específica, sendo responsável pela manutenção do estado de conservação do equipamento e sua devolução imediata ao setor responsável, assim que rescindida ou encerrada sua contratação junto à Organização.
- A necessidade de guarda ou transporte de equipamentos computacionais pelo Fornecedor da Organização deve ser expressamente autorizada pela Organização. Apenas locais de guarda e trânsito destes equipamentos especificados na autorização concedida podem ser utilizados pelo Fornecedor.
- Apenas mídias de guarda e transporte de ativos de informação expressamente autorizadas pela Organização podem ser utilizadas pelo Fornecedor da Organização.
- Não é permitida a guarda de ativos de informação da Organização pelo Fornecedor após o encerramento da atividade contratada, salvo determinação contrária estabelecida em contrato.

5.2. Controle de acesso físico e lógico

- Os Fornecedores devem portar identificação clara e visível (crachá / etiqueta) ou oferecer documentação de identificação pessoal sempre que solicitado.
- Os Fornecedores devem utilizar identificação e autenticação de usuários de sistema concedidos formalmente pela Organização para realização de suas atividades, informando de erros ou acessos que não correspondam ou excedam ao escopo de sua atuação contratada.
- As credenciais de acesso a sistemas disponibilizadas para Fornecedores são de uso intransferível.
- Sistemas de informação fornecidos por Fornecedores da Organização, para uso de colaboradores da Organização devem oferecer autenticação segura e prover meios de rastreabilidade de ações realizadas. A disponibilização ou integração de tais sistemas deve, preferencialmente, utilizar múltiplos fatores (Strong authentication) e, minimamente, conectar-

se aos controladores da Organização por meio de Serviços de Federação do Active Directory (autenticação moderna do Azure AD) para autenticação de usuários.

5.3. Delimitação de perímetro e proteção de segurança física

- Os Fornecedores devem atuar e transitar apenas em locais expressamente autorizados e relacionados a sua atuação contratada.

5.4. Uso aceitável de ativos e recursos

- Os Fornecedores devem utilizar ativos de informação apenas para o propósito relacionado a sua atuação contratada.
- Os Fornecedores não podem reconfigurar ou alterar capacidades e restrições definidas em equipamentos e recursos tecnológicos de propriedade da Organização. Equipamentos e recursos tecnológicos de posse ou propriedade do Fornecedor, utilizados em sua atuação contratada, não devem oferecer riscos e vulnerabilidades. O uso de tais equipamentos pode estar sujeito a inspeção e avaliação da Organização a qualquer tempo e, inclusive, a proibição de uso.

5.5. Análise e garantias de segurança em sistemas de informação fornecidos

- Sistemas de informação fornecidos por Fornecedores, para uso de colaboradores da Organização e / ou seus clientes, devem oferecer garantias de segurança de informação aplicada. Certificados de análises de segurança vigentes, realizadas por entidades terceiras e independentes competentes, devem ser apresentados sempre que solicitado. Adicionalmente, a Organização reserva-se o direito de realizar análises de segurança (scan de vulnerabilidades, testes de penetração ou outro) para manutenção desta garantia de segurança da informação nestes sistemas.

5.6. Recursos Humanos, Interações e Comunicações

- Os Fornecedores devem utilizar apenas recursos humanos (colaboradores) expressamente declarados e autorizados para a prestação das atividades contratadas (mesmo em atividades executadas fora das dependências da Organização).
- As interações entre o Fornecedor e a Organização devem ser realizadas pelos meios e mídias autorizados pela Organização.

- A comunicação e envio de informações deve ocorrer de forma segura, observando os protocolos e aplicativos de comunicação autorizados pela Organização.

5.7. Planos de Continuidade, Desastre ou Situação de Emergência

- Quando acionados em cenário de contingência, ativação de planos de continuidade e/ou recuperação de desastres, os Fornecedores responsáveis por ações de emergência devem priorizar as ações conforme nível de prioridade classificado pela Organização, respeitando os Acordos de Nível de Serviço (ANS) definidos em contrato.
- Caso definido em contrato, os Fornecedores que suportam áreas críticas de negócio devem oferecer, regularmente, resultados de testes de execução de planos de continuidade e/ou recuperação de desastres relacionados aos produtos e serviços escopo do contrato, de forma a demonstrar atendimento ao processo, entregáveis e tempos acordados com a Organização.
- Todas as ações de emergência executadas com a participação do Fornecedor devem obedecer aos princípios de segurança da informação estabelecidos pela Organização.

5.8. Requisitos Legais e Regulamentares adicionais

- Todas as imposições de segurança, adicionais a esta política, determinadas por requisitos Legais ou Regulamentos Setoriais aos quais a Organização estiver submetida, geram obrigação de cumprimento solidário do Fornecedor, limitado a sua atuação contratada.
- Caso o Fornecedor armazene dados da Organização ou de seus Clientes fora do território nacional, deverá informar a Organização do país de armazenamento. A mudança de armazenamento para qualquer outro país diferente do informado inicialmente deve ser previamente consultada e autorizada pela Organização.

5.9. Criptografia, Privacidade e Monitoramento

- O Fornecedor que manusear dados pessoais em detrimento de sua atividade contratada é responsável pela garantia de que esses dados sejam gerenciados de acordo com todas as normas de Privacidade e Proteção de Dados Pessoais aplicáveis.
- Todas as informações confidenciais, com acesso concedido ao Fornecedor devem obedecer aos princípios de segurança e gestão de chaves estabelecidos pela Organização. Não é permitido ao Fornecedor alterar permissões ou interferir na gestão de acesso a informações de propriedade da Organização.
- A Organização se reserva ao direito de monitorar e controlar ações de credenciais providas pela Organização e utilizadas por Fornecedores, assim como inspecionar o conteúdo de

mensagens e comunicações efetuadas por meio do uso da rede de computadores sob responsabilidade da Organização.

5.10. Subcontratação

- O Fornecedor que optar pela subcontratação de parte ou todo o escopo de serviços, deve obter anuência prévia da Organização para tal.
- Caso a subcontratação seja aprovada pela Organização, é responsabilidade do Fornecedor a garantia do conhecimento e cumprimento de todas as diretrizes aqui dispostas pelos subcontratados.

6. REFERÊNCIA A OUTROS DOCUMENTOS

Não se aplica.