Política de Segurança da Informação para Fornecedores

Ref: PSIF V1.0

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

Política de Segurança da Informação para Fornecedores

sodexo
QUALITY OF LIFE SERVICES

Índice

1 – CONSIDERAÇÕES INICIAIS

1.1 – FINALIDADE

Este documento define todas as regras e princípios básicos da Política de Segurança da Informação e de Sistemas que devem ser aplicadas aos fornecedores da Sodexo para garantir, de forma consistente e eficiente, a proteção das Informações disponibilizadas pela Sodexo, incluindo dados sensíveis e pessoais.

Estas instruções são elaboradas e mantidas levando em conta, inclusive, a Segurança dos Sistemas de Informação dos fornecedores e suas infraestruturas que se relacionam com a realização dos serviços prestados à Sodexo. A Política de Segurança da Informação e de Sistemas define os requerimentos que todos os fornecedores devem cumprir para assegurar a devida Gestão de Risco de Segurança das Informações.

1.2 – DIVULGAÇÃO

Este documento é classificado como “Público” e pode ser compartilhado com fornecedores, clientes, órgãos regulatórios e parceiros, conforme necessidade.

1.3 – VERSÕES DO DOCUMENTO

Rev nº	Detalhes da revisão	Data	Cargo
Ver.1.0	Criação do documento	16/01/2018	Analista de Segurança da Informação
Ver.1.0	Revisão inicial	24/01/2018	Especialista em Controles Internos

1.4 – APROVAÇÕES

Aprovado por	
Gerente de Segurança da Informação	03/04/18
Gerente de Controles Internos	03/04/18
Diretor de Riscos, Compliance e Segurança da Informação	03/04/18

2 – CERTIFICAÇÃO DE CONFORMIDADE

A Empresa deverá comprometer-se em checar semestralmente no Portal Web da Sodexo (através do link existente no contrato firmado entre as partes), a atualização desta Política e, certificar sua conformidade através de Carta de Representação.

3 – PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

3.1 - SEGURANÇA DA INFORMAÇÃO DE RECURSOS HUMANOS

PSIFHR 04 – CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- A educação em segurança deve ser um processo contínuo e praticado regularmente a fim de reduzir riscos. Todos os colaboradores do fornecedor de serviços Sodexo que tenham acesso aos sistemas de informação da Sodexo devem acessar, periodicamente e, minimamente de forma anual, um programa de conscientização em segurança e receber notificações periódicas sobre conscientização em segurança.
  Referência: IST-C160.

PSIFHR 06 – RESCISÃO OU MUDANÇA DE RELAÇÃO TRABALHISTA

- Um processo formal deve ser implementado para garantir que, após a rescisão ou mudança de relação trabalhista, os direitos de acesso sejam devidamente e oportunamente removidos ou atualizados, seguindo um processo formal de requisição de mudança.
  É responsabilidade de:
  - Todo o ativo do fornecedor de serviços Sodexo deve ser devolvido pelos seus respectivos colaboradores, incluindo dados, documentos de propriedade intelectual, estações de trabalho e celulares, antes da rescisão ou mudança de relação trabalhista;
  - A Gerência responsável deve garantir que estes ativos sejam devidamente coletados.

Contratos de não-divulgação firmados pelos funcionários e contratados devem permanecer em vigor após a rescisão ou mudança na relação trabalhista.

Referência: IST-C160.

3.2 - GESTÃO DE ATIVOS

PSIFASM 01 – GESTÃO DE ATIVOS

- Os ativos do fornecedor de serviços Sodexo devem ser identificados e um inventário destes ativos deve ser mantido. Os ativos mantidos no inventário devem possuir um proprietário identificado. As normas para o uso aceitável e seguro dos ativos devem ser definidas, documentadas e implementadas.
  Referência: IST-C150; IST-C700.

PSIFASM 03 – CLASSIFICAÇÃO DE INTEGRIDADE DE DADOS

- Os dados devem ser classificados com base nas exigências de integridade de dados. O devido conjunto de medidas para a identificação de tratamento de dados deve estar definido e implementado com base nos critérios internos do fornecedor de serviços Sodexo. Caso não esteja, recomendamos ao fornecedor de serviços Sodexo a implementação e esquema de classificação de dados adotado pela Sodexo, conforme detalhado abaixo:
  Referência: IST-C410.

  Informações Internas:
  São informações que requerem especial atenção antes de qualquer utilização e/ou divulgação.
  Os requerimentos para seu manuseio ou utilização são determinados por sua classificação que pode ter três níveis: Restrita, Confidencial ou Altamente Confidencial.

  Informações Externas:
  As informações externas são informações de domínio público e passível apenas de um nível de classificação: Pública

  São informações públicas aquelas que podem ser acessadas e divulgadas livremente, independente de sua abrangência, cuja divulgação não representa nenhum risco para o negócio.

  Classificação de documentos:
  Os documentos deverão ter, de forma explícita, a classificação da informação a que se referem:

  1) Capa do documento: os documentos Confidenciais e Altamente Confidenciais devem possuir a classificação destacada na capa.

  2) Corpo do Documento: todos os documentos internos (restritos, confidenciais e altamente confidenciais) devem possuir a classificação da informação em seu cabeçalho e rodapé.

PSIFASM 05 – TRATAMENTO DE MÍDIA

- As mídias (discos rígidos internos/externos, drives de memória, etc.) devem ser descartadas de forma segura quando não forem mais exigidas, de acordo com os procedimentos formais, a fim de prevenir a divulgação não autorizada de dados. Em particular, o descarte de mídias utilizadas no armazenamento de dados sensíveis deve ser rastreado e registrado.
  Referência: IST-C360.

3.3 - CONTROLE DE ACESSO

PSIFACC 01 – POLÍTICA DE ACESSO LÓGICO

- O acesso aos ativos deve ser gerenciado pelo proprietário dos ativos. Em particular, as normas de controle de acesso devem ser estabelecidas, documentadas e revisadas periodicamente. O acesso aos dados, sistemas e aplicativos deve ser controlado por um procedimento seguro de autenticação.
  Referência: IST-C010; IST-C020.

PSIFACC 02 – GESTÃO DE IDENTIDADE NOS SISTEMAS DE INFORMAÇÃO

- Todos os usuários, sejam do fornecedor de serviços Sodexo ou das organizações que trabalham com/para este, devem ser identificados individualmente.
  Referência: IST-C020.

PSIFACC 03 – CONTAS NOMINAIS

- Todas as contas de usuário devem ser nominais ou devidamente atreladas a um indivíduo, sem ambiguidade. Uma conta de serviço deve ser tratada como uma conta privilegiada e, atrelada, sem ambiguidade, a um usuário que se responsabilizará por tal conta.
  Referência: IST-C020.

PSIFACC 04 – CONTAS PRIVILEGIADAS

- O acesso às contas privilegiadas deve ser restrito e justificado, e deve ser concedido para uso específico compatível com a descrição do cargo ou operação específica que precisa ser realizada. As contas privilegiadas devem ser revisadas periodicamente, ao menos uma vez por ano. É terminantemente proibido se beneficiar destes direitos de acesso privilegiado para a execução de quaisquer outras operações. Inclui, entre outros, a segurança dos dispositivos de Rede, Sistemas Operacionais, Bancos de dados e Sistemas.
  Referência: IST-C020; IST-C030.

PSIFACC 05 – CONTAS PADRÃO

- As contas padrão não exigidas para a operacionalização do sistema devem ser excluídas ou desativadas após a instalação / implementação do sistema.
- As contas padrão que são exigidas para a operacionalização do sistema ou as que não podem ser excluídas / desativadas devem:
  1) Ser imediatamente configuradas com uma nova senha. Recomendamos a configuração dos parâmetros de senha abaixo:

  - As senhas devem ter no mínimo 8 caracteres e devem conter uma letra maiúscula e um numeral. O
  - identificador não pode ser parte da senha.
  - As senhas irão expirar após 90 dias. Novas senhas devem ser únicas. Senhas que tenham expirado
  - recentemente não podem ser usadas novamente por cinco alterações consecutivas de senha.
  - Após 5 tentativas erradas de log-on, a conta deverá ser desativada.
  - Se o usuário não conseguir lembrar-se de sua senha ou se o usuário achar que alguém pode ter obtido sua senha, ele deverá entrar em contato com a Central de Suporte para obter auxílio.

  2) Ser tratadas como contas privilegiadas *(de acordo com a seção PSIFACC - 04).* Inclui, entre outros, a segurança dos dispositivos de Rede, Sistemas Operacionais, Bancos de dados e aplicativos.
  Referência: IST-C020; IST-C030.

PSIFACC 07 – NORMAS DE PROTEÇÃO DE DADOS CONFIDENCIAIS

- Os usuários são responsáveis pela proteção de suas senhas. Em particular, usuários não devem compartilhar suas senhas com outras pessoas, e devem diferenciar as senhas de trabalho das pessoais. Os usuários não devem utilizar as mesmas senhas em diferentes recursos e não devem utilizar as mesmas senhas ao longo do tempo. As mudanças de senhas devem ser realizadas de forma mandatória nas primeiras autenticações dos usuários.
  Referência: IST-C030; IST-C160.

PSIFACC 08 – GUARDA DE CREDENCIAIS COM ACESSO PRIVILEGIADO

- A guarda de credenciais com acessos privilegiados deve ser realizada através de um processo formal, a fim de garantir suas características de confidencialidade. Em particular, a equipe responsável pela Segurança da Informação deve garantir que qualquer transmissão de senha de usuário seja feita através de um canal seguro de comunicação. A identificação (login) e a autenticação (senha) não devem ser repassadas aos usuários através do mesmo canal de comunicação.
  Referência: IST-C030.

PSIFACC 10 – CONTROLE DE ACESSO DE APLICAÇÃO E RECURSO

- Um procedimento deve definir o papel do dono da informação ou dono do sistema para que o processo de concessão de acesso a estas informações passe por sua respectiva aprovação. Este procedimento deve se aplicado a todos os usuários, incluindo administradores (usuários privilegiados). Adicionalmente, casos de emergência também devem passar por este processo.
  Referência: IST-C020.

PSIFACC 11 – GESTÃO DE ACESSO DE USUÁRIO

- Os processos de gestão de acesso de usuário devem ser definidos e formalizados, incluindo as etapas de provisionamento, alteração e exclusão. O acesso de usuário deve ser atribuído conforme necessário e deve ser aprovado pela alçada apropriada de sua respectiva gestão.
  O processo deve garantir a responsabilização pelas ações de gestão de acesso de usuário. Revisões formais de direitos de acesso de usuário devem ser realizadas em intervalos regulares, dependendo da criticidade do ativo, no mínimo uma vez por ano, a fim de identificar qualquer acesso não autorizado e garantir a devida segregação de atribuições.
  Referência: IST-C020; IST-C040;

PSIFACC 12 – SEGREGAÇÃO DE ACESSO EM FUNÇÕES DE TI

- A equipe não-operacional não deve ter acesso aos ativos produtivos, salvo se aprovado em caso de acesso específico e temporário. Em particular, a equipe de desenvolvimento não deve ter acesso aos ambientes de teste e produção. As atividades de desenvolvimento de aplicativo e as atividades de implementação de aplicativo/pacote devem ser segregadas. Se possível, as funções administrativas de sistema e rede devem ser independentes em relação às funções de análise de segurança e monitoramento do registro. A segregação de acesso deve ser definida e validada. Os direitos de acesso de usuário devem ser concedidos de acordo com a segregação de acesso.
  Referência: IST-C040; IST-C230.

3.4 - SEGURANÇA FÍSICA

PSIFPHY 01 – PERÍMETRO DE SEGURANÇA FÍSICA E PROTEÇÃO DE EQUIPAMENTOS

- O acesso físico às áreas de segurança deve ser restrito ao pessoal autorizado. Os equipamentos devem ser protegidos, e sua localização deve ser identificada. Medidas de proteção contra desastres ambientais devem ser implementadas de acordo com os riscos relevantes. Mecanismos de detecção devem ser implementados para atuar frente a riscos de desastre e invasão.
  Referência: IST-C150; IST-C151.

PSIFPHY 02 – CONTROLES DE ACESSO FÍSICO

- As áreas de segurança devem ser protegidas por controles de acesso apropriados, a fim de garantir que apenas o pessoal autorizado será capaz de acessar os ativos sensíveis.
  Referência: IST-C151

PSIFPHY 03 – UTILITÁRIOS DE SUPORTE

- Os servidores e dispositivos de rede devem ser protegidos contra quedas de energia e outras interrupções causadas por falhas nos utilitários de suporte, tais como água, combustível de geradores, etc.
  Referência: IST-C150

PSIFPHY 05 – MANUTENÇÃO DE EQUIPAMENTOS

- Todos os ativos de TI devem ser corretamente mantidos para garantir sua disponibilidade e integridade contínuas.
  Referência: IST-C090; IST-C150.

PSIFPHY 06 – GARANTIA DE PROTEÇÃO DOS EQUIPAMENTOS DE TI PELOS SEUS USUÁRIOS

- Os usuários devem seguir as seguintes recomendações para garantir a devida proteção de seus equipamentos. É recomendado:
  - Encerrar as sessões ativas assim que concluídas, salvo se houver a possibilidade de proteção por um mecanismo de bloqueio apropriado;
  - Desconectar de aplicativos ou serviços de rede quando não for mais necessário;
  - Proteger os computadores ou dispositivos móveis de uso não autorizado, por meio de trava de chave ou controle equivalente.

  Dispositivos móveis (laptop, tablet, smartphone) devem ser protegidos, e as opções relevantes de proteção são criptografia de disco/dispositivo, varredura remota, geolocalização, etc.
  Referência: IST-C090.

PSIFPHY 07 – POLÍTICA DE LIMPEZA DE AMBIENTE DE TRABALHO

- A política de ambiente de trabalho limpo, sem papéis e dados removíveis de armazenamento, e a política de tela limpa nas instalações de processamento de informações devem ser adotadas levando com conta as classificações de dados, exigências legais e contratuais e riscos. Em particular, recomendamos que:
  - Informações corporativas sensíveis devem ser bloqueadas;
  - Computadores devem ter suas sessões encerradas ou protegidas por um mecanismo de bloqueio de sessão quando não tiverem seus usuários presentes, protegidos por senha, ou por outro mecanismo relevante de autenticação;
  - Chaves eletrônicas de acesso e tokens de segurança não devem ser deixados sem usuário presente;
  - Mídias contendo informações sensíveis devem ser removidas de impressoras imediatamente.
- *Referência: IST-C090; IST-C160.*

3.5 - SEGURANÇA DE OPERAÇÕES E COMUNICAÇÃO

PSIFOPE 01 – GESTÃO DE MUDANÇAS

- O desenvolvimento de um novo Sistema de Informação e/ou alterações no Sistema de Informação existente (sistemas operacionais, aplicações) pode implicar em novos riscos. Tais modificações devem se submeter a

um processo formal e rígido de gestão de mudanças, incluindo a avaliação de risco de Segurança de Sistemas de Informação.
Referência: IST-C010; IST-C200.

PSIFOPE 02 – ACESSO À TI DA SODEXO

- Ativos que não sejam do fornecedor de serviços Sodexo não devem ser conectados diretamente à Rede Corporativa Privada do fornecedor de serviços Sodexo. Se um terceiro exigir acesso a uma Rede Corporativa Privada, este terceiro deverá utilizar o equipamento do fornecedor de serviços Sodexo ou deverá ser alocado em uma área dedicada da infraestrutura em que as devidas medidas de proteção sejam implementadas. O risco associado ao acesso ao Sistema de Informação por terceiros deve ser identificado e avaliado, e os devidos controles de segurança devem ser implementados antes da concessão de tal acesso.
  Referência: IST-C060.

PSIFOPE 03 – CONTROLES DE REDE

- As redes devem ser gerenciadas e controladas para proteger as informações de sistemas e aplicativos.
  Referência: IST-C060; IST-C070.

PSIFOPE 04 – SEGURANÇA DE SERVIÇOS DE REDE

- Cada serviço de rede, seja local ou terceirizado, deve incluir mecanismos de segurança (proteção, detecção e reação) adaptados à sensibilidade dos dados sendo transmitidos. Estes mecanismos de segurança devem ser implementados na rede ou diretamente nos sistemas, aplicativos, estações de trabalho ou banco de dados.
  Referência: IST-C060; IST-C070.

PSIFOPE 05 – CONEXÃO LOCAL COM A REDE CORPORATIVA PRIVADA

- Todas as conexões locais à rede corporativa interna do fornecedor de serviços Sodexo devem ser protegidas por firewall, com os devidos registros para fins de monitoramento geral.
  Referência: IST-C060.

PSIFOPE 06 – INTERCONEXÕES COM REDES NÃO CORPORATIVAS

- Todas as interconexões entre a rede corporativa do fornecedor de serviços Sodexo e redes não corporativas *(Internet, terceiros, parceiros, consórcios, entre outros)* devem incluir a proteção, detecção e reação dos mecanismos de segurança.
  Referência: IST-C060.

PSIFOPE 09 – ACESSO REMOTO

- O acesso remoto aos Sistemas de Informação do fornecedor de serviços da Sodexo deve ser protegido, recomendamos os seguintes controles:
  - Criptografia de comunicação até chegar na rede corporativa privada;
  - Autenticação forte;
  - Disponibilidade de registros de conectividade.

  O acesso remoto aos Sistemas de Informação do fornecedor de serviços da Sodexo não deve diminuir a segurança da rede corporativa.
  Referência: IST-C070.

PSIFOPE 10 – BRIDGING

- A conexão de um ativo simultaneamente a uma rede corporativa e a uma rede não corporativa, criando assim uma ponte entre as duas redes, não é recomendada, com exceção feita aos dispositivos de segurança desenvolvidos especificamente para interconectar várias redes.
  Referência: IST-C070.

PSIFOPE 13 – TRANSFERÊNCIA DE DADOS

- Todas as transferências de dados devem ser realizadas por ferramentas explicitamente validadas pela equipe responsável de Segurança da Informação do fornecedor de serviços Sodexo. A transferência de dados através de plataformas públicas (Dropbox, Wetransfer, entre outros) não é recomendada.
  Referência: IST-C410.

PSIFOPE 14 – CONTRATOS DE TRANSFERÊNCIA DE DADOS

- A transferência de dados de informações corporativas entre o fornecedor de serviços Sodexo e as partes externas devem ser definidas e formalizadas antes de qualquer tipo de transferência. O processo deve ser inspecionado pela equipe responsável pela Segurança da Informação do fornecedor de serviços Sodexo.
  Referência: IST-C410.

PSIFOPE 15 – SEGURANÇA DE TRANSFERÊNCIA DE DADOS

- Todos os sistemas de transferência de dados (e-mail, compartilhamento de arquivos, transferência de dados entre aplicativos, etc.…) devem incluir os devidos meios de proteção de transmissão e armazenamento de dados, com a garantia da confidencialidade, integridade, disponibilidade e responsabilidade com base nos níveis de classificação das informações.
  Referência: IST-C410.

PSIFOPE 16 – PROTEÇÃO DE ENDPOINT

- Todos os ativos corporativos (estações de trabalho, servidores, dispositivos móveis, etc.) devem contar com proteção contra-ataques e ameaças (fraude, phishing, vírus, worm, ransomware e outros malwares), incluindo e, não se limitando a software malicioso e ataques na rede, através do uso de medidas e controles preventivos, de detecção e de recuperação devidamente atualizados. Em particular, os endpoints devem possuir pelo menos um software antivírus ativo e atualizado. Recomendamos a proteção dos dispositivos móveis corporativos através de uma solução de Gestão de Dispositivo Móvel (“MDM”).
  Referência: IST-C090.

PSIFOPE 20 – REGISTRO DE EVENTOS

- Ações realizadas nos ativos de TI devem ser registradas, centralizadas e, tais registros devem ser revisados regularmente. Esta regra deve ser aplicada a equipamentos de rede, Sistemas Operacionais, middleware, banco de dados e aplicações.
  Referência: IST-C010; IST-C420.

PSIFOPE 21 – MONITORAMENTO DE SEGURANÇA

- Os sistemas de Informações de Segurança e Gestão de Evento (“SIEM”) garantem a segurança da centralização dos registros de eventos, proteção contra manipulação/acesso não autorizados e permitem a correlação do registro para fins de detecção de incidente de segurança. Recomendamos que os registros de eventos de segurança possam ser gerenciados por meio de uma solução de SIEM.
  Referência: IST-C420.

PSIFOPE 22 – GESTÃO DE CORREÇÕES

- Todos os sistemas do fornecedor de serviços Sodexo (estações de trabalho, servidores, dispositivos de rede, etc.) devem contar com os devidos níveis de correção de segurança atualizados. Recomendamos a elaboração de um procedimento formal para gerir este processo. Adicionalmente, recomendamos que vulnerabilidades críticas de segurança possam ser corrigidas no prazo de um mês a contar da publicação da correção. Este processo deve incluir um procedimento de repetição para a restauração para o último estado estável conhecido. Para sistemas que não podem ser corrigidos, as devidas proteções e monitoramento de segurança específicos devem ser adotados de acordo com a classificação de segurança do ativo.
  Referência: IST-C400.

PSIFOPE 23 – DETECÇÃO, AVALIAÇÃO E REMEDIAÇÃO DE VULNERABILIDADE

- As informações sobre vulnerabilidades técnicas de sistemas de TI em utilização devem ser obtidas tempestivamente e a exposição a tais vulnerabilidades deve ser avaliada com as devidas medidas sendo adotadas para o tratamento do risco associado.
  Referência: IST-C400.

PSIFOPE 24 – BACKUP DE INFORMAÇÕES E SISTEMAS

- As políticas de backup devem ser definidas para os dados, software e sistemas de acordo com as exigências do negócio. Os backups devem ser devidamente realizados e testados. Recomendamos o armazenamento do backup de forma “offline” para prevenir a manipulação não autorizada de sistemas comprometidos e em local remoto para prevenir a destruição juntamente com a fonte primária dos dados.
  Referência: IST-C350; IST-C360.

3.6 - AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMA

PSIFSYS 01 – SEGURANÇA NO CICLO DE VIDA DO PROJETO

- Sempre que o fornecedor de serviços Sodexo iniciar um novo projeto de TI ou mudança substancial em sistema de informação existente, recomendamos que os itens obrigatórios de segurança sejam documentados, tais como: Questionário de avaliação de risco de segurança, análise de risco, testes e outros documentos relevantes.
  Referência: IST-C220; IST-C250; IST-C700.

PSIFSYS 02 – AVALIAÇÃO E MEDIDAS DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- Para cada novo projeto, um Questionário de Avaliação de Risco de Segurança deve ser preenchido e as medidas de segurança implementadas devem ser identificadas.
  Referência: IST-C250.

PSIFSYS 03 – ACEITAÇÃO DE RISCO RESIDUAL

- Durante o projeto, os riscos residuais devem ser identificados e precisam ser formalmente aceitos pelas partes interessadas. Esta aceitação deve ser documentada em um registro de risco residual.
  Referência: IST-C250.

PSIFSYS 04 – TESTES

- Na fase de testes, os atributos de segurança devem ser testados e as ações específicas de segurança devem ser adotadas para validar tecnicamente o nível de segurança do projeto.

Referência: IST-C220.

PSIFSYS 09 – GESTÃO DE TERCEIROS

- Os projetos entregues por terceiros devem estar de acordo com controles de segurança adotados pelo fornecedor de serviços Sodexo.
  Referência: IST-C700.

PSIFSYS 11 – SEGURANÇA DE REDE

- Os controles de segurança de rede aplicados nos projetos devem estar de acordo com controles de segurança adotados pelo fornecedor de serviços Sodexo.
  Referência: IST-C070; IST-C230.

3.7 - RELAÇÕES COM TERCEIROS

PSIFSPL 01 – CLÁUSULAS DE SEGURANÇA EM CONTRATOS DE FORNECIMENTO

- Os contratos com prestadores de serviço devem cumprir com os princípios da Política de Segurança da Informação do fornecedor de serviços Sodexo. As exigências e condições de segurança devem ser definidas e implementadas, em particular, recomendamos que os controles abaixo sejam aplicados:
  - Incluir as exigências de segurança;
  - Definir como estas exigências são monitoradas;
  - Permitir a auditoria das exigências de segurança da informação pelo fornecedor de serviços Sodexo ou sua contratada;
  - Fazer menção a uma cláusula de reversão protegendo os interesses do fornecedor de serviços Sodexo.
- Se o contrato com prestadores de serviço especificar exigências e condições de segurança para o fornecedor de serviços Sodexo, a equipe responsável pela segurança da informação do fornecedor de serviços Sodexo deve ser envolvida antes da assinatura do contrato, a fim de avaliar sua relevância e eficácia.
  Referência: IST-C700.

3.8 - GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

PSIFINC 01 – IDENTIFICAÇÃO E GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- Os incidentes de Segurança da Informação e de Sistemas devem ser identificados e gerenciados por processos consistentes, disciplinados e compartilhados. Em particular, recomendamos:
  - Os incidentes devem ser classificados por tipo e gravidade de incidente;
  - A gravidade do incidente deve ser reavaliada regularmente;
  - Os canais de alerta e comunicação devem ser identificados;
  - Os papéis e a responsabilidade devem ser atribuídos de acordo com a gravidade;
  - Os recursos a serem mobilizados para a gestão do incidente devem ser identificados.
- No caso de um incidente de Segurança da Informação e de Sistemas, a equipe responsável pela Segurança da Informação do fornecedor de serviços Sodexo deve realizar a coordenação do esforço coletivo até que o

incidente seja declarado encerrado. Todos os gestores do fornecedor de serviços Sodexo são responsáveis pela alocação de seus recursos até que o incidente seja encerrado.
Referência: IST-C010; IST-C340.

PSIFINC 02 – COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- Assim que identificados e, o mais rápido possível, todos os incidentes de segurança devem ser notificados e comunicados através de canais oficiais apropriados. Este tipo de conscientização deve ser realizado pela equipe de segurança da informação do fornecedor de serviços Sodexo aos seus respectivos colaboradores.
  Referência: IST-C340.

PSIFINC 03 – OBTENÇÃO DE EVIDÊNCIA

- Devem ser definidos e aplicados procedimentos de identificação, coleta, aquisição e preservação de informações, que podem servir como evidência. Em particular, os procedimentos de gestão de incidente devem garantir a obtenção destas evidências e, adicionalmente, no que diz respeito a uma eventual solicitação de por parte de uma atividade/análise forense.
  Referência: IST-C340.

PSIFINC 04 – GESTÃO DE CRISE DE SEGURANÇA

- A organização e os processos de gestão de crise de segurança devem ser definidos e testados regularmente.
  Referência: IST-C340.

PSIFINC 05 – APRENDENDO COM OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- O conhecimento adquirido com a análise e resolução de incidentes de Segurança da Informação e de Sistemas deve ser utilizado para reduzir a probabilidade ou o impacto de incidentes futuros.
  Referência: IST-C340.

3.9 - PLANO DE RECUPERAÇÃO DE DESASTRE

PSIFDRP 01 – EXIGÊNCIAS DE DRP

- Recomendamos que as exigências do Plano de Recuperação de Desastre (“DRP”) sejam definidas de acordo com o Objetivo do Tempo de Recuperação (“RTO”) e Objetivo de Ponto de Recuperação (“RPO”) para cada componente de Sistema da Informação. Em particular, estas exigências devem cumprir com as obrigações regulatórias e de clientes. O RTO e o RPO devem ser definidos e validados com base na Avaliação de Impacto no Negócio (“BIA”), realizada por cada entidade.
  Referência: IST-C280.

PSIFDRP 02 – ESTRATÉGIA DE DRP

- As exigências de DRP devem ser observadas por meio de uma estratégia definida e documentada de DRP validada pela alta gerência do fornecedor de serviços Sodexo. Em particular e, no que diz respeito ao Datacenter, este deve possuir uma estratégia de DRP definida, implementada e documentada.
  Referência: IST-C280.

PSIFDRP 03 – COBERTURA DE DRP

- O DRP deve ser implementado em caso de desastres, principalmente por meio de medidas preventivas, detectoras e corretivas.

Referência: IST-C280.

PSIFDRP 04 – IMPLEMENTAÇÃO DE DRP

- Os ativos de suporte de Sistemas da Informação devem ser implementados com redundância suficiente para cumprir com as exigências de disponibilidade.
  Referência: IST-C280.

PSIFDRP 05 – TESTES E MANUTENÇÃO DE DRP

- O DRP deve ser mantido e testado pelo menos uma vez por ano para garantir suas premissas. Os cenários de teste devem ser relevantes e incluir os casos de uso end-to-end, envolvendo usuários comerciais.
  Referência: IST-C280.

3.10 - CONFORMIDADE

PSIFCPL 01 – PLANO DE CONTROLE DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- Um plano anual de controle de Segurança da Informação e de Sistemas deve ser definido e realizado com o propósito de controlar o nível geral de Segurança da Informação e de Sistemas e a observância das políticas de Segurança da Informação e de Sistemas.
  Referência: IST-C380.

PSIFCPL 02 – OBSERVÂNCIA DAS POLÍTICAS E NORMAS DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS

- As atividades comerciais devem regularmente revisar a observância do processamento e procedimentos de informação em sua área de responsabilidade com as respectivas políticas, normas e quaisquer outras exigências de Segurança da Informação e de Sistemas.
  Referência: IST-C160.

PSIFCPL 03 – REVISÃO DE CONFORMIDADE TÉCNICA

- As políticas de Segurança da Informação e de Sistemas devem ser revisadas regularmente.
  Referência: IST-C380.

PSIFCPL 05 – OBSERVÂNCIA DE LEIS E NORMAS

- As atividades do fornecedor de serviços Sodexo devem garantir a observância das obrigações estatutárias e regulatórias para assegurar que as devidas exigências de segurança sejam levadas em conta em seus processos. Todas as exigências legais, estatutárias e regulatórias relevantes devem ser explicitamente definidas e documentadas para os novos processos de Segurança da Informação e de Sistemas, ou soluções a serem desenvolvidas ou aprimoradas.
  Referência: IST-C600.

PSIFCPL 06 – OBSERVÂNCIA DAS NORMAS E LEIS DE PRIVACIDADE DE DADOS

- O proprietário de dados é responsável pela garantia de que os dados pessoais sejam gerenciados de acordo com todas as normas de Proteção de Dados Pessoais. Os dados pessoais devem ser mantidos de acordo com as leis e normas locais aplicáveis, e de acordo com as diretrizes do Grupo e diretrizes legais e regulatórias locais.
  Referência: IST-C600.

PSIFCPL 07 – OBSERVÂNCIA DE INSTRUMENTOS CONTRATUAIS

- As atividades da empresa devem garantir a observância das obrigações contratuais para assegurar que as devidas exigências de segurança sejam levadas em conta em seus processos.
  Referência: IST-C600.

PSIFCPL 09 – VIOLAÇÕES

- No caso de violação da presente política, a gerência responsável deve aplicar quaisquer medidas internas relevantes e notificar a equipe de Segurança da Informação. Qualquer evento que resultar em roubo, perda, uso não autorizado, divulgação não autorizada, destruição não autorizada, ou serviços degradados ou recusados de ativos da Informação do fornecedor de serviços Sodexo implica uma violação da Segurança da Informação e de Sistemas. As violações podem incluir, entre outros, qualquer ato que exponha o fornecedor de serviços Sodexo a lucros cessantes potenciais ou efetivas devido ao comprometimento da segurança dos ativos de Sistemas da Informação da Sodexo, que envolva a divulgação de informações sensíveis ou confidenciais, ou o uso não autorizado de dados ou ativos do fornecedor de serviços Sodexo, que envolva o uso de Sistemas da Informação para benefício próprio ou em fins não éticos, danosos ou ilícitos, ou que afetem negativamente a reputação ou marca do parceiro de negócio. Se julgado necessário, ações disciplinares, civis ou penais (não exclusivas) podem ser adotadas em caso de violação.
  Referência: IST-C380.