DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ELABORADO POR:	RAFAEL LEITÃO	REV:	00
APROVADO POR:	MARCELO LIMA		
DISCIPLINA:	SEGURANÇA DA INFORMAÇÃO	DATA:	30/11/23

1. OBJETIVO

O objetivo desta Instrução Técnica é estabelecer e especificar requisitos e condições necessárias para a gestão da Segurança da Informação no ambiente da **Toyo Setal**. Tem como propósito definir processos, visando manter a ocorrência e o impacto de incidentes de segurança da informação em níveis aceitáveis em relação ao apetite de risco corporativo.

2. REFERÊNCIAS

ISO/IEC 27001 - Sistema de Gestão da Segurança da Informação.

Nota: A norma citada deve ser utilizada em sua versão mais recente

3. TERMOS E DEFINIÇÕES

Ativo de Informação: são todos os dispositivos que produzem, processam, transmitem ou armazenam informações, ou a própria informação em si, tais como: informações como segredos de negócios, relatórios impressos, documentos eletrônicos, profissionais, certificados digitais, equipamentos de telecomunicações, computadores, *smartphones*, etc.

Sistemas de Informação: um sistema de informação é um conjunto organizado de elementos, podendo ser pessoas, dados, atividades ou recursos materiais em geral, por exemplo: e-mail, rede, *internet*, dispositivo, VPN, sistemas e/ou aplicações corporativas. Estes elementos interagem entre si para processar informação de forma adequada em função dos objetivos da empresa.

Proprietário da Informação: é o responsável pela criação, classificação, concessão, revisão e manutenção a determinado conjunto de informações em sistemas, e-mail e documentos digitais e físicos. O proprietário identificado não tem necessariamente quaisquer direitos de propriedade sobre o ativo de informação.

Área Custodiante: é a área responsável pelos aspectos funcionais e operacionais de um determinado tipo de item de configuração (ativo). Tem responsabilidade sobre tarefas operacionais delegadas pelo proprietário do ativo. Entende-se por áreas custodiantes da Gerência de Tecnologia da Informação, todas as suas áreas internas.

Responsável pelo prestador de serviço: é o gestor do contrato ou profissional autorizado por ele.

Classificação da Informação: a classificação da informação consiste na atribuição do nível de sigilo e a indicação de seu respectivo rótulo pelo Proprietário da Informação para determinar quais controles devem ser aplicados, visando preservar a informação.

Termo de Responsabilidade de Segurança da Informação: é o documento cujo conteúdo define as regras de Segurança da Informação que os profissionais devem seguir.

Acordo de Confidencialidade: é uma cláusula contratual firmada entre a **Toyo Setal** e empresas terceiras, visando garantir a confidencialidade das informações.

Drive de Rede: área virtual remota que tem como objetivo o armazenamento de arquivos lógicos.

Antivírus: software responsável por identificar e bloquear arquivos nocivos e códigos maliciosos (vírus) no ambiente de Sistemas de Informação.

Códigos Maliciosos: são programas de computador projetados especificamente para atentar contra a segurança dos sistemas computacionais, normalmente através da exploração de vulnerabilidades, com objetivos de infiltrar-se e espalhar-se automaticamente, causando danos, apagando dados, roubando informações, divulgando serviços, etc.

Comitê de Segurança da Informação (COSI): grupo formado com a missão de discutir questões relacionadas à segurança da informação e os riscos associados ao negócio.

Controle de Segurança da Informação: medida que modifica o risco. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que mudam o risco. É possível que os controles nem sempre exerçam a modificação pretendida ou presumida aos riscos, gerando assim o que é conhecido como risco residual.

Risco Residual: é a quantidade de risco que permanece ou que aparece após a inclusão dos controles adicionais e/ou ajustes dos controles existentes.

Matriz de Riscos: documento que estabelece a implementação de um controle de segurança da informação ou projeto de melhoria de segurança da informação, ou que formaliza a aceitação do risco.

4. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

As diretrizes de Segurança da Informação podem ser definidas como declarações formais da **Toyo Setal** acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, e tem como principal objetivo formalizar a abordagem relacionada à Segurança da Informação na empresa.

O Sistema de Gestão de Segurança da Informação possui as diretrizes de segurança da informação abaixo:

1. Preservar a confidencialidade, integridade e disponibilidade das informações tratadas na administração geral da **Toyo Setal** e empreendimentos por ela administrados;

2. Manter o padrão internacional de Segurança da Informação perante a ISO/IEC 27001;

3. Atender aos requisitos aplicáveis de segurança da informação de acordo com o negócio;

4. Melhorar continuamente o Sistema de Gestão da Segurança da Informação;

5. Minimizar os riscos de violações ou perdas de quaisquer ativos de tecnologia da informação;

6. Desenvolver e aperfeiçoar os recursos humanos e tecnológicos sob o Sistema de Gestão da Segurança da Informação.

5. RESPONSABILIDADES

a) Da área de Segurança da Informação

- Administrar o Sistema de Gestão de Segurança da Informação.
- Propor e apoiar iniciativas que visem a segurança dos ativos de informação da **Toyo Setal**, de acordo com as recomendações dos órgãos reguladores;
- Promover a atualização da Política de Segurança da Informação aprovada pelo Comitê de Segurança da Informação;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- Analisar em conjunto com a área de Tecnologia da Informação e/ou Gerências envolvidas nos incidentes de segurança da informação e propor as ações para o tratamento das vulnerabilidades, conforme a análise dos riscos;
- Manter comunicação efetiva com o Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do comitê ou de membros da diretoria;
- Auditar rotineiramente os controles de segurança da informação;
- Monitorar atividade de todos os usuários durante os acessos às redes, inclusive *internet* (sites visitados e e-mails recebidos/enviados), com o objetivo de identificar comportamentos maliciosos;
- Apoiar as auditorias internas e/ou externas e realizar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Identificar preventivamente e mitigar riscos que comprometem a segurança da informação e de serviços em ambiente corporativo;
- Realizar estudo, implementar e administrar solução/ferramenta a ser aplicada no ambiente para elevar o nível da Segurança da Informação;
- Executar ações de controle e gestão de mecanismo/ferramentas de segurança cibernética;
- Realizar gestão de vulnerabilidade em sistemas, dispositivos e infraestrutura disponibilizados na rede interna e externa e adequar os serviços que necessitam de controles de segurança.

b) Do Comitê de Segurança da Informação

- Atuar de acordo com o estabelecido no Regimento Interno do Comitê de Segurança da Informação.
- Avaliar material disponibilizado mensalmente pelo Analista de Segurança da Informação;

- Avaliar os riscos, incidentes e vulnerabilidades de segurança e propor ações corretivas;
- Sempre que for necessário, discutir sobre algum incidente grave ou relevante para a **Toyo Setal** e fazer recomendações ao Diretor de Governança e Integridade;
- O COSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

c) Dos Gestores das áreas internas da Toyo Setal

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os profissionais sob a sua gestão (liderança e comprometimento);
- Informar à área de Segurança da Informação o desligamento de prestadores de serviço, incluindo terceiros em formato de “Pessoa Jurídica”;
- Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação das diretrizes, procedimentos e/ou de suas instruções técnicas.

d) Dos Profissionais das diversas áreas

- Cumprir as Políticas de Segurança da Informação;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Assinar o Termo de Responsabilidade de Segurança da Informação, formalizando a ciência e o aceite da Política de Segurança da Informação, bem como assumindo a responsabilidade por seu cumprimento;
- Proteger as informações contra acessos, modificações, destruições ou divulgações não autorizadas;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelas diretrizes e procedimentos da empresa;
- Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação dos procedimentos de segurança da informação.

e) Da Tecnologia da Informação

- Garantir a recuperação dos dados corporativos, além de administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes;
- Gerar e manter as trilhas para auditoria de acordo com as especificações estabelecidas para rastrear possíveis falhas e fraudes nos sistemas críticos do Plano de Continuidade dos Sistemas de Informação;

- Configurar os equipamentos e sistemas concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança da informação corporativa;
- Garantir que todos os servidores, computadores e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios, acessar os arquivos e dados de outros usuários. No entanto, esta ação somente será permitida quando da execução de atividades exclusivas de sua rotina de trabalho que exijam tal acesso, como, por exemplo, a manutenção de computadores, realização de cópias de segurança ou testes no ambiente. O acesso deverá ser devidamente autorizado e documentado.
- Quando ocorrer a troca de computador de qualquer usuário, garantir que as informações do usuário anterior sejam removidas de forma irrecuperável antes de disponibilizar o ativo para próximo usuário;
- O processo de aquisição e desenvolvimento de sistemas e acesso em produção deve atender requisitos de segurança previsto nas especificações de segurança da **Toyo Setal**.

f) Da área de Suprimentos

- Incluir a cláusula de segurança da informação como parte integrante de todos os contratos de prestação de serviço.

g) Da área de Segurança Patrimonial

- Criar mecanismos de proteção para ativos de informação nos locais físicos da empresa.

h) Da área de Desenvolvimento Humano e Organizacional / Recursos Humanos e Administração de Pessoal

- Fazer com que todo profissional, ao ser admitido, assine o Termo de Responsabilidade de Segurança da Informação da **Toyo Setal**.
- Comunicar imediatamente à área de Segurança da Informação toda e qualquer demissão, bem como promoções e demais mudanças de cargo e área, contendo nome e matrícula.

i) Da área de Privacidade e Proteção de Dados

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os profissionais da empresa;

- Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação das diretrizes, procedimentos e/ou de suas instruções técnicas;
- Conduzir, junto à área de Segurança da Informação, plano de ação quando houver incidentes de segurança da informação que envolvam dados pessoais.

6. DIRETRIZES ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO

As diretrizes específicas de Segurança da Informação foram definidas como desdobramento das diretrizes gerais, no que tange à implementação dos controles aplicáveis de segurança da informação:

- **Tratamento da Informação**: A **Toyo Setal** deve criar, gerir e avaliar critérios de tratamento e classificação das informações que lhe pertencem, ou estejam sob sua responsabilidade, de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor e demais normas aplicáveis.

- **Gestão de Incidentes**: Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, de forma a impedir a interrupção das atividades da empresa e não afetar negativamente o alcance dos seus objetivos estratégicos.

- **Gestão de Riscos**: Foi estabelecido um processo de Gestão de Riscos de Segurança da Informação, com a finalidade de minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

- **Gestão de Continuidade**: A Gestão de Continuidade de Negócio foi estabelecida no âmbito da **Toyo Setal**, visando reduzir a possibilidade de interrupção das atividades e serviços, causada por desastres ou falhas graves nos recursos tecnológicos que suportam as operações críticas.

- **Controle de Acessos Lógicos**: Foram formalizadas regras que estabeleçam procedimentos, garantam o controle de acesso às informações, instalações e sistemas de informação, fazendo uso de mecanismos de verificação e de um segundo fator de autenticação, quando aplicável.

- **Controle de Acessos Físicos, Segurança Física e Segurança do Ambiente**: Os ativos da empresa são protegidos contra acesso físico de pessoas não autorizadas, bem como contra danos, perdas, furto e interferências internas e externas. As proteções estão alinhadas aos riscos identificados relacionados ao ativo.

- **Armazenamento, Descarte e Transporte Seguros da Informação**: Foram estabelecidos procedimentos seguros, com os mecanismos apropriados, que garantem a segurança das informações tratadas pela **Toyo Setal**, sejam elas físicas ou digitais, garantindo a segurança e inviolabilidade de seu conteúdo, evitando que pessoas não autorizadas tenham acesso às mesmas.

- **Classificação da Informação**: Foi estabelecida uma classificação sistemática e objetiva para qualificar as informações que circulem no âmbito da **Toyo Setal**, considerando a sua importância para o desenvolvimento das atividades da empresa, a necessidade de proteção à privacidade das pessoas às quais os dados se referem a criticidade, a sensibilidade e relevância da informação.

- **Uso de dispositivos próprios *(Bring Your Own Device - BYOD)***: A **Toyo Setal** se reserva ao direito de deletar as informações de propriedade da empresa em dispositivos perdidos ou de profissionais que não tenham mais vínculo com a empresa. No caso da utilização de dispositivos pertencentes à **Toyo Setal**, estes serão monitorados e as informações pertencentes à empresa serão preservadas. As informações da empresa não devem ser acessadas através de dispositivos que não são de propriedade da empresa, exceto sob autorização expressa da Gestão de Segurança da Informação ou fornecimento de meio de acesso controlado pela empresa.

- **Código de Conduta**: O **Código de Conduta** é pertinente apenas aos profissionais que atuam diretamente na **Toyo Setal**, dispensando fornecedores, clientes e terceiros. Todos os profissionais da **Toyo Setal** assinam o Código de Conduta.

- **Orientação para Autenticação**: Para a criação de senhas seguras, recomenda-se adotar minimamente o uso de (08) oito caracteres, os quais são compostos por números e letras. Não devem ser utilizadas senhas de fácil associação aos usuários, como data de nascimento, sobrenome, números de telefone, nome de cônjuges etc.

  No caso de o usuário não utilizar o segundo fator de autenticação, este terá o acesso bloqueado após 05 (cinco) tentativas incorretas e precisará abrir uma solicitação na ferramenta de abertura de chamados. Além disso, não é permitido o uso de gerenciadores de senhas não homologados pela **Toyo Setal**. Para garantir maior segurança, também deve ser utilizado o segundo fator de autenticação sempre que o sistema ou aplicação permitir.

- **Gestão de *Backups***: Para assegurar o bom funcionamento da gestão de *backups*, determina-se que os sistemas sejam classificados de acordo com sua criticidade e tenham rotinas de *backup* compatíveis com o apetite a risco do negócio. Os *backups* devem ser monitorados pelos responsáveis e sua execução deve ser evidenciada. Ainda, para preservar a confiabilidade do processo de restauração, deve-se adotar testes de restauração periódicos, que simulem um incidente para que seja necessário restabelecer o ambiente ao estado original. Esta simulação deve ser executada em ambiente de testes, para evitar que sejam sobrescritos os arquivos contidos no ambiente de produção.

- **Gestão de Mudanças Tecnológicas**: A gestão de mudanças no âmbito da TI é necessária para garantir que os métodos e procedimentos padronizados mais adequados sejam utilizados para o manuseio eficiente de todas as alterações ocorridas no ambiente organizacional da **Toyo Setal**.

  As mudanças devem ser propostas através de formulário específico que detalhe: escopo, janela de execução, plano de execução e plano de restauração. Este formulário deve passar por um aprovador, ser registrado na ferramenta de abertura de chamados e as evidências de sua execução devem ser anexadas.

- **Homologação de Aplicações**: Para garantir a segurança e bom funcionamento dos ativos de informação da **Toyo Setal**, somente aplicações e softwares aceitos pela empresa poderão ser instalados e executados nos notebooks, VDIs (*Virtual Desktop Infrastructure*) e outros sistemas de uso dos profissionais. Quaisquer outros softwares serão, a princípio, bloqueados, mas sua execução ou instalação pode ser aceita mediante solicitação via ferramenta de abertura de chamados.

- **Homologação de Serviços em Nuvem**: Para garantir a homologação correta e funcional dos serviços em nuvem, somente serviços aceitos pela empresa poderão ser utilizados pelos profissionais.

O uso de outros serviços será, a princípio, negado, considerando que os ambientes dispõem de dados que são frequentemente consultados ou atualizados. Além disso, possuem altos requisitos de tempo de resposta de acesso e a preservação destes ambientes se faz necessária. No entanto, a utilização de outras soluções, sistemas ou serviços não listados pode ser aceita mediante solicitação via ferramenta de abertura de chamados, após realizados os testes em ambiente isolado.

- **Trabalho remoto**: O trabalho remoto, quando autorizado, só é permitido com a utilização de dispositivos de propriedade da **Toyo Setal**. Estes serão monitorados e as informações pertencentes à empresa serão preservadas.

  Os profissionais em trabalho remoto devem usar o seu login corporativo para acessar os sistemas necessários para o desenvolvimento do seu trabalho, não sendo permitido o uso de login anônimo. O login é pessoal e intransferível, não podendo ser compartilhado com outros usuários ou revelado a qualquer pessoa, de maneira que todas as atividades realizadas possam ser rastreadas e identificadas.

  O desenvolvimento das atividades em trabalho remoto deve ter a mesma diligência e seguir as mesmas regras de segurança aplicadas no trabalho presencial. Os cuidados em relação à exposição indevida de informações, principalmente em relação às confidenciais e dados pessoais, devem ser realizados da mesma forma que são realizados no trabalho presencial. A informação não deve ficar exposta em cima de mesas ou ser armazenada em locais inseguros e sem vigilância.

  O equipamento/dispositivo fornecido pela **Toyo Setal** deverá sempre ser bloqueado na ausência temporária do profissional, bem como desligado ao final da jornada de trabalho.

7. SANÇÕES E PUNIÇÕES

As seguintes sanções e punições são aplicáveis aos respectivos casos descritos:

- As violações desta política e/ou demais normas e procedimentos de segurança, mesmo que por mera omissão ou tentativa não consumada, são passíveis das penalidades previstas na Política de Medidas Disciplinares da **Toyo Setal**.

- A aplicação de sanções e punições deve ser realizada conforme a recomendação do Comitê de Segurança da Informação, com base na Política de Medidas Disciplinares da **Toyo Setal**.

- Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano à **Toyo Setal**, o infrator deve ser responsabilizado pelos prejuízos conforme previsto nas normas internas, cabendo, ainda, aplicação das medidas judiciais pertinentes.

- Os casos omissos devem ser avaliados pelo Comitê de Segurança da Informação para posterior recomendação, conforme a Política de Medidas Disciplinares da **Toyo Setal**.

As diretrizes estabelecidas nessa política e nas demais normas e procedimentos da Segurança da Informação não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da **Toyo Setal** adotar, sempre que possível, outras medidas de segurança além daquelas que aqui estão previstas, com o objetivo de garantir proteção as informações da **Toyo Setal**.

8. PADRÕES APLICÁVEIS

SQ-00-SSI-01-FOR-01	Termo de Responsabilidade de Segurança da Informação