MANUAL SGPI - ANALISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

SANTOS PORT AUTHORITY

SUMÁRIO

MANUAL SGPI – ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃOE E PRIVACIDADE

1. DISPOSIÇÕES INICIAIS

Fica instituído o Manual de Análise e Avaliação de Riscos de Segurança da Informação e Privacidade, apoio ao Sistema de Gestão de Privacidade da Informação (SGPI), como parte integrante do conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação e melhoria contínua do SGPI.

A SPA tendo iniciado em março de 2020 o projeto de adequação à LGPD, optou por adotar para o assunto, o processo de análise e avaliação de riscos de SI&P especificado no documento “Projeto de Adequação da SPA à LGPD”, no qual estabelece, entre outras, as normas ISO de segurança como referência para adoção de medidas organizacionais para a segurança e privacidade da informação, estabelecendo no âmbito da SPA, a abrangência para todos os processos e setores que envolvam informações e, em especial, dados pessoais.

A estrutura de decisão da SPA está descrita na “Política de Segurança e Privacidade, e SGPI”

2. OBJETIVO E ABRANGÊNCIA

O presente Manual tem por objetivo definir as regras de elaboração do relatório de Análise e Avaliação de Riscos de Segurança da Informação e Privacidade da SPA.

Este manual trata da avaliação técnica e específica dos riscos relacionados à segurança da informação e privacidade, não abrangendo a avaliação de riscos corporativos e de processos tratados em normativos próprios.

Os riscos de segurança da informação e privacidade, presumem, em consonância com a norma ISO-27005, uma abordagem baseada na valoração dos ativos de informação anterior as considerações de probabilidade e impacto.

Esta avaliação de riscos adota em sua análise dos ativos uma valoração quantitativa, baseada em critérios CID estendido para Privacidade (CID&P), vide Anexo II – Tabela de Pesos para CID&P.

Esta análise e avaliação destina-se à:

- Suportar o SGPI da SPA, materializado no documento "Declaração de Aplicabilidade" (também conhecido como SoA);
- Prover conformidade legal e evidência de avaliação de riscos de SI&P;
- Contribuir para a continuidade de negócios;
- Contribuir para a avaliação de riscos corporativos;
- Contribuir para preparação/execução de plano de resposta a incidentes.

A aplicação deste Manual, acompanha a definição de escopo presente na POLÍTICA DE SEGURANÇA E PRIVACIDADE E SGPI.

3. DEFINIÇÕES

Para os fins deste Manual são adotados os seguintes conceitos:

- **SoA:** Declaração de Aplicabilidade, do inglês "*Statement of Aplicability*". Documento resultante de uma avaliação de Riscos de Segurança e Privacidade, onde se encontram os controles (baseados nas normas ISO 27701/27001/27002), aplicáveis para mitigação de riscos de Segurança da Informação e Privacidade (SI&P).
- **Risco:** Efeito da incerteza nos objetivos. Em segurança da Informação está associado com o potencial de que ameaças possam explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, consequentemente, causar danos a uma organização, e pode ser expresso em termos de combinação de consequências

(impactos) de um evento e a probabilidade associada da ocorrência. (ref. ISO-27005).

- **Análise de Riscos:** processo de compreender a natureza do risco e determinar o nível de risco (ref. ISO-27005).
- **Nível de risco:** magnitude de um risco expressa em termos da combinação das consequências (ou impacto) e de suas probabilidades (ref. ISO-27005).
- **Avaliação de riscos:** processo de comparar os resultados da análise de riscos com critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável (ref. ISO-27005).
- **Processo de avaliação de riscos:** processo global de identificação de riscos, análise de riscos e avaliação de riscos (ref. ISO-27005).
- **CID&P:** acrônimo para Confidencialidade, Integridade, Disponibilidade & Privacidade. CID, também é conhecida como a pilares da Segurança da Informação.
- **Cenários de Risco:** trata-se de 37 cenários de riscos (proposto no Risk-IT Framework da ISACA de riscos)
-

4. REFERÊNCIAS

4.1. Lei nº13.709/2018 – Lei Geral de Proteção de Dados.

4.2. Decreto nº 9.637/ 2018 - Institui a Política Nacional de Segurança da Informação.

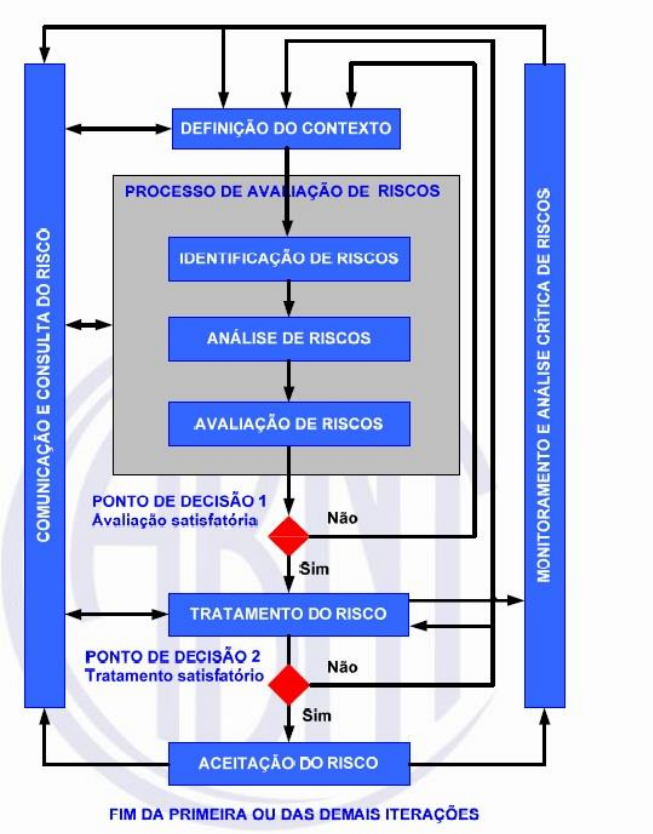
4.3. ISO 27001 *Information technology -- Security techniques - Information security management systems – Requirements* (Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação - Requisitos)

4.4. ISO 27701 *Information technology -- Security techniques – Privacy Information Management System* (PIMS) (Tecnologia da Informação –

Técnicas de Segurança – Sistema de Gestão da Privacidade da Informação – SGPI).

4.5. ISO 27005 *Information technology --Security techniques - Information security risk management* (Tecnologia da Informação –Técnicas de Segurança – Gerenciamento Riscos Segurança Informação)

5. PROCESSO DE AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE



Processo de gestão de riscos de segurança da informação

5.1. O processo de avaliação de riscos, leva em consideração:

5.1.1. A importância do ponto de vista operacional dos processos e dos negócios, da disponibilidade, da confidencialidade e da integridade, e privacidade.

5.1.2. As expectativas e percepções das partes interessadas e consequências negativas para o funcionamento do negócio SPA.

5.1.3. A valoração dos ativos de informação envolvidos, baseado no valor CID&P, pelas áreas responsáveis por meio da soma dos pesos, conforme "Anexo II - Tabela de Pesos Para CID&P". O valor resultante guarda relação com a criticidade do ativo de informação.

5.1.4. Caso a valoração do ativo atinja o valor mínimo de 8 (caso contrário o ativo não possui importância suficiente para ser considerado no processo):

5.1.4.1. Identificação de cenários de risco (baseado no *Risk It Framework – ISACA*), pelas áreas responsáveis, aplicáveis a cada ativo.

5.1.4.2. Identificação da probabilidade e impacto de eventos de SI&P (indicados pelos cenários de risco) pelas áreas responsáveis.

5.1.4.3. Valoração da probabilidade x impacto para definição de nível de risco.

5.1.4.4. Identificação dos controles existentes para tratamento do risco.

5.2. CRITÉRIO DE ACEITAÇÃO DE RISCO

5.2.1. Conforme o valor quantitativo do risco obtido nas tabelas do Anexo III – Tabelas de Probabilidade, Impacto e Nível de Risco, aceita-se os riscos conforme tabela do Anexo IV – Tabela de Classificação/tratamento de riscos.

5.3. CRITÉRIOS DE PROBABILIDADE E IMPACTO

5.3.1. Conforme o valor CID&P ou criticidade do ativo (se igual ou superior a 8, obtido a partir da soma dos respectivos pesos), identifica-se os cenários de risco e respectivos níveis de probabilidade e impacto;

5.3.2. Os níveis de probabilidade e impacto estão descritos nas tabelas do Anexo III – Tabelas de Probabilidade, Impacto e Nível de Risco com as respectivas pontuações.

5.4. IDENTIFICAÇÃO DOS RISCOS DE SI&P

5.4.1. São os riscos relacionados à perda de Confidencialidade, Integridade, Disponibilidade e Privacidade.

5.4.2. A lista de cenários (Anexo I – Tabela de Cenários de Risco), deve ser considerada para a identificação dos riscos de SI&P.

5.4.3. Para cada ativo de informação sujeito a identificação de riscos, pode ser aplicável mais de um cenário de risco. A utilização de cenários de risco deve ser considerada ao invés de identificação de ameaças e vulnerabilidades, para cada ativo;

5.5. ANÁLISE DE RISCO DE SI&P

5.5.1. VARIÁVEIS ENVOLVIDAS NA ANÁLISE DE RISCO

5.5.1.1. Considera-se na avaliação todos os ativos sob gestão da Superintendência de TI (SUPTI), agrupados conforme sua natureza específica e destacados conforme importância no processo de negócio.

5.5.1.2. A valoração dos ativos deve ser efetuada segundo os critérios CID&P conforme “Anexo II - Tabela de Pesos para CID&P”;

5.5.1.3. Para simplificar, poderão ser utilizados os Cenários de Risco (*Risk-IT Framework* da ISACA), em substituição à definição de ameaças e vulnerabilidades, conforme “Anexo I - Tabela de Cenários de Riscos”

5.5.1.4. Controles existentes para tratamento de riscos.

5.5.1.5. Determinação de probabilidade e impacto conforme Anexo III – Tabelas de Probabilidade, Impacto e Nível de Risco.

5.5.2. AVALIAÇÃO DOS IMPACTOS E PROBABILIDADE

5.5.2.1. Cada ativo em conjunto com o cenário de risco aplicável ao ativo será pontuado conforme sua probabilidade e seu impacto de acordo com a tabela do Anexo III – Tabelas de Probabilidade, Impacto e Nível de Risco.

5.5.2.2. Considerar históricos e estatísticas quando aplicável.

5.5.3. **DETERMINAÇÃO DO NÍVEL DE RISCO**

5.5.3.1. Pela multiplicação das pontuações de probabilidade e impacto obtém-se o nível de risco a ser considerado na avaliação de risco considerando as opções de tratamento, em consonância com o Anexo IV – Tabela de Classificação/Tratamento de Risco.

5.6. **AVALIAÇÃO DE RISCOS DE SI&P**

5.6.1.1. Comparar os valores de nível de risco com os critérios de aceitação ao risco (Anexo IV – Tabela de Classificação/Tratamento de Risco).

5.6.1.2. Se houver vários riscos a serem tratados, estes devem ser priorizados para tratamento, em sequência, de acordo com seu nível de risco. Esta análise apresentará um valor quantitativo em que há a indicação do controle, a partir dos cenários e valor risco relativos a cada ativo, incluindo os controles da ISO-27001, aplicáveis. Esse valor quantitativo é um indicativo de priorização, que pode ser complementado por outros fatores.

6. TRATAMENTO DE RISCOS

6.1. Os resultados da avaliação suportarão elementos para publicar uma Declaração de Aplicabilidade (Anexo VIII – Modelo de SoA), que elenca os controles da norma. Cada risco deve ser tratado individualmente em conformidade com os objetivos de SI&P.

6.2. **OPÇÕES DE TRATAMENTO**

6.2.1. São opções a serem consideradas na determinação do tratamento de risco, conforme Anexo IV – Tabela de Classificação/Tratamento de Risco:

6.2.1.1. Mitigar

6.2.1.2. Transferir

6.2.1.3. Rejeitar

6.2.1.4. Aceitar

6.3. **DETERMINAÇÃO DE CONTROLES NECESSÁRIOS**

6.3.1. Cada controle deve ser determinado com base nas informações de risco de SI&P resultantes da avaliação de riscos e nos controles da ISO 27701 e do anexo A da ISO 27001.

6.3.2. Os controles determinados e não determinados devem compor o SoA, sendo que para os não aplicáveis, deve haver uma justificativa e para os demais, considerando que são necessários, deve haver uma indicação de implementação (totalmente implementado, em andamento, não iniciado)

7. PLANO DE TRATAMENTO DE RISCOS

7.1. Como resultado do processo de avaliação de riscos, um plano de tratamento deve ser estabelecido em documento que conste (vide Anexo IX - Modelo de plano de tratamento de risco):

7.1.1. Os riscos identificados;

7.1.2. Opções de tratamento;

7.1.3. Controles necessários;

7.1.4. Estado de implementação;

7.1.5. Responsável pelo tratamento ou proprietário do risco.

8. MONITORAMENTO E ANÁLISE CRÍTICA DE RISCOS

8.1. O plano de tratamento de riscos deverá orientar o estabelecimento de planos de ação que podem impactar na gestão de mudanças.

8.2. O resultado dessas ações, bem como a materialização de riscos, contribuirá para novas revisões das avaliações de risco.

8.3. O Comitê de Segurança da Informação (CSI), deve ter elementos para fazer uma avaliação crítica dos riscos de segurança e situação no decorrer do processo de tratamento.

8.4. As revisões, tanto das avaliações como do presente manual deverão ser anuais ou em função de ação que o justifique.

9. PAPÉIS E RESPONSABILIDADES

9.1. O processo de Análise e Avaliação De Riscos De Segurança Da Informação e Privacidade, deve ser conduzido pela área de Segurança da Informação e Privacidade da SPA, considerando as informações necessárias fornecidas pelas áreas consideradas no escopo do processo.

10. COMUNICAÇÃO E CONSULTA DOS RISCOS DE SI&P

10.1. Conforme evolução dos trabalhos, as informações sobre os riscos de SI&P devem ser comunicadas pela área de Segurança da Informação e Privacidade ao Comitê de Segurança da Informação e a Diretoria Executiva.

11. DISPOSIÇÕES FINAIS

11.1. Os casos omissos no presente Manual devem ser analisados pela SUPTI.

ANEXO I - Tabela de Cenários de Risco

Número cenário	Descrição
1	Seleção de programas de TI
2	Novas tecnologias
3	Seleção de tecnologia
4	Tomada de decisão de investimento em TI
5	Prestação de contas sobre TI
6	Integração da TI nos processos de negócios
7	Estado de tecnologia de infraestrutura
8	Envelhecimento do software de aplicativos
9	Agilidade arquitetônica e flexibilidade
10	Conformidade regulatória
11	Implementação de software
12	Término do projeto de TI
13	Economia de projetos de TI
14	Entrega de projetos
15	Qualidade do projeto
16	Seleção/desempenho de fornecedores terceirizados
17	Roubo de infraestrutura
18	Destruição da infraestrutura
19	Equipe de TI
20	Experiência e habilidades de TI
21	Integridade do software
22	Infraestrutura (hardware)
23	Desempenho do software
24	Capacidade do sistema
25	Envelhecimento do software infra estrutural
26	Malware
27	Ataques lógicos
28	Mídia de informação
29	Desempenho dos utilitários
30	Ação industrial
31	Integridade de dados (base)
32	Invasão lógica
33	Erros operacionais de TI
34	Conformidade contratual
35	Ambiental
36	Atos da natureza
37	LGPD

ANEXO II - Tabela de Pesos Para CID&P

Peso	Confidencialidade	Integridade	Disponibilidade	Privacidade
3 (Alto)	As informações armazenadas ou tratadas no ativo são classificadas como confidenciais/secreta	A integridade do ativo, da informação armazenada ou tratada nele é crítica para o processo de negócio	A disponibilidade do ativo é crítica para o processo de negócio	Violações de privacidade no ativo, da informação tratada ou armazenada nele tem grande impacto negativo para os titulares de dados pessoais e para a empresa
2 (Médio)	As informações armazenadas ou tratadas no ativo são classificadas como interna	A falta de integridade do ativo, da informação armazenada ou tratada nele gera impactos negativos para o processo de negócios	A falta de disponibilidade gera impactos negativos para o processo de negócios	Violação de privacidade tem impacto negativo mediano para os titulares de dados pessoais e para a empresa
1 (Baixo)	As informações armazenadas ou tratadas são de uso públicas	A falta de integridade do ativo, da informação armazenada ou tratada nele gera ineficiência, mas não tem impactos significativos sobre o processo de negócio	A falta de disponibilidade gera ineficiência, mas não tem impactos significativos sobre o processo de negócios	Violações de privacidade tem pouco impacto negativo para os titulares de dados pessoais e para a empresa

ANEXO III – Tabelas de Probabilidade, Impacto e Nível de exposição ao Risco

Os parâmetros escalares adotados neste documento para Probabilidade são apresentados na tabela a seguir:

Classificação	Valor	Descrição
Alto	4	É muito provável/certamente que o risco ocorra
Provável	3	É provável que o risco ocorra
Possível	2	É possível que o risco ocorra
Remoto	1	É remota a probabilidade de o risco ocorrer

Os parâmetros escalares adotados neste documento para Impacto são apresentados na tabela a seguir:

Classificação	Valor	Descrição
Muito Alto	4	É muito alto o impacto caso o risco ocorra
Alto	3	É alto o impacto caso o risco ocorra
Médio	2	É médio o impacto caso o risco ocorra
Baixo	1	É baixo o impacto caso o risco ocorra

Matriz de risco ou Mapa de calor: Probabilidade x Impacto, considerado o instrumento de apoio para a definição dos critérios de classificação do nível de risco.

PROBABILIDADE					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		IMPACTO			

ANEXO IV - Tabela de classificação/tratamento de riscos

Classificação Risco	Valores	Ação para tratamento do risco
Muito Alto	12,16	Mitigar (eliminar, transferir, reduzir)
Alto	8,9	Mitigar (eliminar, transferir, reduzir)
Médio	3,4,6	Mitigar (eliminar, transferir, reduzir)
Baixo	1,2	Aceitar

ANEXO V - Exemplo tabela de ativos

Descrição	Gestor	Tipo Ativo	Confidencialidade	Integridade	Disponibilidade	Privacidade	Valor Ativo CID&P
Notebook	GERID	Hardware	3	3	3	3	12
Desktop	GERID	Hardware	3	3	3	3	12
Switch	GERID	rede	3	3	3	3	12

ANEXO VI - Tabela tipo de ativos

Tipo de ativo	Primário/Suporte
processos e atividades do negócio	Primário (PRIM)
informação	Primário (PRIM)
hardware	Suporte (SUPORTE)
software	Suporte (SUPORTE)
rede	Suporte (SUPORTE)
recursos humanos	Suporte (SUPORTE)
instalações físicas	Suporte (SUPORTE)
estrutura da organização	Suporte (SUPORTE)

ANEXO VII – Exemplo de tabela de análise de risco

Ativo de Inf	C	I	D	P	valor	Cenário risco	Controles existentes	Prob. (P)	Impacto (I)	val risco P x I	tratar
Notebook, gestor:GERID, tipo:hardware	3	3	3	3	12	Seleção de tecnologia		3	3	9	sim
						Estado de tecnologia de infraestrutura		3	3	9	sim
						Roubo de infraestrutura		3	2	6	sim
						Destruição da infraestrutura		2	3	6	sim
						Malware		2	3	6	sim
						Ataques lógicos		3	3	9	sim
						Invasão lógica		3	3	9	sim
Desktop, gestor:GERID, tipo:hardware	3	3	3	3	12	Tomada de decisão de investimento em TI		2	4	8	sim
						Implementação de software		1	4	4	não
						Roubo de infraestrutura		1	3	3	não
						Destruição da infraestrutura		1	3	3	não
						Ataques lógicos		2	3	6	sim
						Invasão lógica		2	3	6	sim
						Ambiental		1	3	3	não
Switch, gestor:GERID, tipo:rede	3	3	3	3	12	Novas tecnologias		1	1	1	não
						Roubo de infraestrutura		1	2	2	não
						Destruição da infraestrutura		1	3	3	não
						Desempenho do software		2	4	8	sim
						Ataques lógicos		1	4	4	não
						Invasão lógica		1	4	4	não

ANEXO VIII - Modelo de SoA (Declaração de Aplicabilidade)

Item ISO-27701 (base 27001)	Aplicável (Sim/Não)	Justificativa	Status implementação	Documento de referência/Evidência
5-Políticas de Segurança da Informação				
5.1-Orientação da direção para segurança da informação				
5.1.1-Políticas para segurança da informação				
5.1.2-Análise crítica das políticas para segurança da informação				
6-Organização da Segurança da Informação				
6.1-Organização interna				
6.1.1-Responsabilidades e papéis pela segurança da informação				
6.1.2-Segregação de funções				
6.1.3-Contato com autoridades				
6.1.4-Contato com grupos especiais				
6.1.5-Segurança da informação no gerenciamento de projetos				
6.2-Dispositivos móveis e trabalho remoto				
6.2.1-Política para o uso de dispositivo móvel				
6.2.2-Trabalho remoto				
7-Segurança em Recursos Humanos				
7.1-Antes da contratação				
7.1.1-Seleção				
7.1.2-Termos e condições de contratação				
7.2-Durante a contratação				
7.2.1-Responsabilidades da direção				
7.2.2-Conscientização, educação e treinamento em segurança da informação				
7.2.3-Processo disciplinar				
7.3-Encerramento e mudança da contratação				
7.3.1-Responsabilidades pelo encerramento ou mudança da contratação				
8-Gestão de ativos				
8.1-Responsabilidade pelos ativos				
8.1.1-Inventário dos ativos				
8.1.2-Proprietário dos ativos				
8.1.3-Uso aceitável dos ativos				
8.1.4-Devolução de ativos				
8.2-Classificação da informação				
8.2.1-Classificação da informação				
8.2.2-Rótulos e tratamento da informação				

8.2.3-Tratamento dos ativos				
8.3-Tratamento de mídias				
8.3.1-Gerenciamento de mídias removíveis				
8.3.2-Descarte de mídias				
8.3.3-Transferência física de mídias				
9-Controle de acesso				
9.1-Requisitos do negócio para controle de acesso				
9.1.1-Política de controle de acesso				
9.1.2-Acesso às redes e aos serviços de rede				
9.2-Gerenciamento de acesso do usuário				
9.2.1-Registro e cancelamento de usuário				
9.2.2-Provisionamento para acesso de usuário				
9.2.3-Gerenciamento de direitos de acesso privilegiados				
9.2.4-Gerenciamento da informação de autenticação secreta de usuários				
9.2.5-Análise crítica dos direitos de acesso de usuário				
9.2.6-Retirada ou ajuste de direitos de acesso				
9.3-Responsabilidades dos usuários				
9.3.1-Uso da informação de autenticação secreta				
9.4-Controle de acesso ao sistema e à aplicação				
9.4.1-Restrição de acesso à informação				
9.4.2-Procedimentos seguros de entrada no sistema (log-on)				
9.4.3-Sistema de gerenciamento de senha				
9.4.4-Uso de programas utilitários privilegiados				
9.4.5-Controle de acesso ao código-fonte de programas				
10-Criptografia				
10.1-Controles criptográficos				
10.1.1-Política para o uso de controles criptográficos				
10.1.2-Gerenciamento de chaves				
11-Segurança Física e do Ambiente				
11.1-Áreas seguras				
11.1.1-Perímetro de segurança física				
11.1.2-Controles de entrada física				
11.1.3-Segurança em escritórios, salas e instalações				

11.1.4-Proteção contra ameaças externas e do meio-ambiente				
11.1.5-Trabalhando em áreas seguras				
11.1.6-Áreas de entrega e de carregamento				
11.2-Equipamentos				
11.2.1-Escolha do local e proteção do equipamento				
11.2.2-Utilidades				
11.2.3-Segurança do cabeamento				
11.2.4-Manutenção dos equipamentos				
11.2.5-Remoção de ativos				
11.2.6-Segurança de equipamentos e ativos fora das dependências da organização				
11.2.7-Reutilização e alienação segura de equipamentos				
11.2.8-Equipamento de usuário sem monitoração				
11.2.9-Política de mesa limpa e tela limpa				
12-Segurança nas operações				
12.1-Responsabilidades e procedimentos operacionais				
12.1.1-Documentação dos procedimentos de operação				
12.1.2-Gestão de mudanças				
12.1.3-Gestão de capacidade				
12.1.4-Separação dos ambientes de desenvolvimento, teste e de produção				
12.2-Proteção contra códigos maliciosos				
12.2.1-Controles contra códigos maliciosos				
12.3-Cópias de segurança				
12.3.1-Cópias de segurança das informações				
12.4-Registros e monitoramento				
12.4.1-Registros de eventos				
12.4.2-Proteção das informações dos registros de eventos (logs)				
12.4.3-Registros de eventos (log) de administrador e operador				
12.4.4-Sincronização dos relógios				
12.5-Controle de software operacional				
12.5.1-Instalação de software nos sistemas operacionais				
12.6-Gestão de vulnerabilidades técnicas				
12.6.1-Gestão de vulnerabilidades técnicas				

12.6.2-Restrições quanto à instalação de software				
12.7-Considerações quanto à auditoria de sistemas de informação				
12.7.1-Controles de auditoria de sistemas de informação				
13-Segurança nas comunicações				
13.1-Gerenciamento da segurança em redes				
13.1.1-Controles de redes				
13.1.2-Segurança dos serviços de rede				
13.1.3-Segregação de redes				
13.2-Transferência de informação				
13.2.1-Políticas e procedimentos para transferência de informações				
13.2.2-Acordos para transferência de informações				
13.2.3-Mensagens eletrônicas				
13.2.4-Acordos de confidencialidade e não divulgação				
14-Aquisição, desenvolvimento e manutenção de sistemas				
14.1-Requisitos de segurança de sistemas de informação				
14.1.1-Análise e especificação dos requisitos de segurança da informação				
14.1.2-Serviços de aplicação seguros em redes públicas				
14.1.3-Protegendo as transações nos aplicativos de serviços				
14.2-Segurança em processos de desenvolvimento e de suporte				
14.2.1-Política de desenvolvimento seguro				
14.2.2-Procedimentos para controle de mudanças de sistemas				
14.2.3-Análise crítica técnica das aplicações após mudanças nas plataformas operacionais				
14.2.4-Restrições sobre mudanças em pacotes de Software				
14.2.5-Princípios para projetar sistemas seguros				
14.2.6-Ambiente seguro para desenvolvimento				
14.2.7-Desenvolvimento terceirizado				
14.2.8-Teste de segurança do sistema				
14.2.9-Teste de aceitação de sistemas				
14.3-Dados para teste				
14.3.1-Proteção dos dados para teste				

15-Relacionamento na cadeia de suprimento				
15.1-Segurança da informação na cadeia de suprimento				
15.1.1-Política de segurança da informação no relacionamento com os fornecedores				
15.1.2-Identificando segurança da informação nos acordos com fornecedores				
15.1.3-Cadeia de suprimento na tecnologia da comunicação e informação				
15.2-Gerenciamento da entrega do serviço do fornecedor				
15.2.1-Monitoramento e análise crítica de serviços com fornecedores				
15.2.2-Gerenciamento de mudanças para serviços com fornecedores				
16-Gestão de incidentes de segurança da informação				
16.1-Gestão de incidentes de segurança da informação e melhorias				
16.1.1-Responsabilidades e procedimentos				
16.1.2-Notificação de eventos de segurança da informação				
16.1.3-Notificando fragilidades de segurança da informação				
16.1.4-Avaliação e decisão dos eventos de segurança da informação				
16.1.5-Resposta aos incidentes de segurança da informação				
16.1.6-Aprendendo com os incidentes de segurança da informação				
16.1.7-Coleta de evidências				
17-Aspectos da segurança da informação na gestão da continuidade do negócio				
17.1-Continuidade da segurança da informação				
17.1.1-Planejando a continuidade da segurança da informação				
17.1.2-Implementando a continuidade da segurança da informação				
17.1.3-Verificação, análise crítica e avaliação da continuidade da segurança da informação				
17.2-Redundâncias				
17.2.1-Disponibilidade dos recursos de processamento da informação				
18-Conformidade				
18.1-Conformidade com requisitos legais e contratuais				
18.1.1-Identificação da legislação aplicável e de requisitos contratuais				
18.1.2-Direitos de propriedade intelectual				
18.1.3-Proteção de registros				

18.1.4-Proteção e privacidade de informações de identificação pessoal				
18.1.5-Regulamentação de controles de criptografia				
18.2-Análise crítica da segurança da informação				
18.2.1-Análise crítica independente da segurança da informação				
18.2.2-Conformidade com as políticas e procedimentos de segurança da informação				
18.2.3-Análise crítica da conformidade técnica				
Item ISO-27701 Clausula 7 Anexo A - Controlador	Aplicável	Justificativa (caso não aplicável)	Status implementação	
7.2-Condições para coleta e processamento				
7.2.1-Identificação e documentação de propósito				
7.2.2-Identificação de bases legais				
7.2.3-Determinação de quando e como o consentimento será obtido				
7.2.4-Obtenção e registro do consentimento				
7.2.5-Análise de impacto de privacidade				
7.2.6-Contrato com processadores de PII				
7.2.7-*Joint PII controller*				
7.2.8-Registros relacionados ao processamento de PII				
7.3-Obrigações para com os PII principais				
7.3.1-Determinando e cumprindo obrigações legais para com os PII principais				
7.3.2-Determinando informações para os PII principais				
7.3.3-Provendo informações para os PII principais				
7.3.4-Provendo mecanismos para modificar ou retirar o consentimento				
7.3.5-Provendo mecanismos para objeção de processamento de PII				
7.3.6-Acesso, correção e/ou exclusão				
7.3.7-Obrigações do PII controller de informar terceiros (t*hird parties*)				
7.3.8-Provendo cópia de PII processada				
7.3.9-Lidando com requisições				
7.3.10-Tomada de decisão automatizada				
7.4-Privacy by design e privacy by default				
7.4.1-Limitação de coleta				

7.4.2-Limitação de processamento				
7.4.3-Exatidão e qualidade				
7.4.4-Objetivos de minimização (anonimização e peudominização)				
7.4.5-Desidentificação (anonimização e pseudonimização) e exclusão de PII ao final do processamento				
7.4.6-Arquivos temporários				
7.4.7-Retenção				
7.4.8-Descarte				
7.5-Compartilhamento, transferência e divulgação de PII				
7.5.1-Identificação dos termos para transferência de PII entre jurisdições				
7.5.2-Países e organizações internacionais para os quais PII podem ser transferidas				
7.5.3-Registro de transferência de PII				
7.5.4-Registro de divulgação de PII para terceiros (*third parties)*				
Item ISO-27701 Clausula 8 Anexo B - Processador	Aplicável	Justificativa (caso não aplicável)	Status implementação	
8.2-Condições para coleta e processamento				
8.2.1-Acordo com cliente (*customer*)				
8.2.2-Propósito da organização				
8.2.3-Uso para propaganda e marketing				
8.2.4-Informação de violação de direitos				
8.2.5-Obrigações do cliente (customer)				
8.2.6-Registros relacionados ao processamento de PII				
8.3-Obrigações para com os PII principals				
8.3.1-Obrigações para com os PII principals				
8.4-Privacy by design e privacy by default				
8.4.1-Arquivos temporários				
8.4.2-Retorno, transferência e descarte de PII				
8.4.3-Controles de transmissão (envio) de PII				
8.5-Compartilhamento, transferência e divulgação de PII				
8.5.1-Identificação dos termos para transferência de PII entre jurisdições				
8.5.2-Países e organizações internacionais para os quais PII podem ser transferidas				
8.5.3-Registro de divulgação de PII para terceiros (third parties)				

8.5.4-Notificação de requisições de divulgação de PII				
8.5.5-Divulgação de PII por obrigação legal				
8.5.6-Divulgação de subcontratados utilizados para processar PII				
8.5.7-Envolvimento de um subcontratado no processamento de PII				
8.5.8-Mudança de subcontratado para processamento de PII				

ANEXO IX - Modelo de plano de tratamento de risco

Ativo de Inf	Cenário risco	Opções de tratamento	Controles Necessários	Estado de implementação	Responsável pelo tratamento ou proprietário do risco
Notebook, gestor:GERID, tipo:hardware	Seleção de tecnologia				
	Estado de tecnologia de infraestrutura				
	Roubo de infraestrutura				
	Destruição da infraestrutura				
	Malware				
	Ataques lógicos				
	Invasão lógica				
Desktop, gestor:GERID, tipo:hardware	Tomada de decisão de investimento em TI				
	Implementação de software				
	Roubo de infraestrutura				
	Destruição da infraestrutura				
	Ataques lógicos				
	Invasão lógica				
	Ambiental				
Switch, gestor:GERID, tipo:rede	Novas tecnologias				
	Roubo de infraestrutura				
	Destruição da infraestrutura				
	Desempenho do software				
	Ataques lógicos				
	Invasão lógica				

INFORMAÇÕES DE CONTROLE

TÍTULO

MANUAL SGPI - ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

VERSÃO

001

UNIDADE GESTORA DO DOCUMENTO

Superintendência de Tecnologia da Informação

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

N/A – Primeira versão

RELAÇÃO COM OUTROS NORMATIVOS

Política de Gestão de Riscos

Política de Segurança e Privacidade e SGPI;

Regulamento Interno de Pessoal da SPA.

Código de Ética e de Conduta e Integridade;

Instrumento Normativo Sistema de Gestão Da Privacidade da Informação: Gestão de Ativos.

NORMATIVOS REVOGADOS

N/A

INSTÂNCIA DE APROVAÇÃO

CONSELHO DE ADMINISTRAÇÃO, 647ª REUNIÃO REALIZADA EM 14/10/2022, POR MEIO DA DELIBERAÇÃO CONSAD Nº 121.2022.