POLÍTICA INSTITUCIONAL N0

1. INTRODUÇÃO

1.1. Sobre a Segurança da Informação

A Informação, nos dias atuais é tratada como um ativo e tal qual deve ser protegida, controlada e monitorada, inclusive pode, em alguns casos, constituir o bem mais valioso da organização pública/privada, visto ser necessário milhares de horas e de pessoas para ser gerada e mantida.

Por si só ela já justifica a atenção especial dedicada. Infelizmente, quando se trata de Segurança da Informação, o prejuízo contabilizado quando algo "não funciona como deveria" não fica restrito a simples perda ou vazamento da Informação, mas em todo o processo na qual ela está envolvida. Assim, salvaguardar os princípios básicos da Segurança da Informação é obrigação inerente ao responsável pela mesma ou pelo processo na qual ela é objeto.

Com este intuito, nos baseamos na "Tríade" postular da Segurança da Informação para construir uma Política que norteie as atividades da Prefeitura e dos Órgãos da Administração Direta e Indireta.

1.2. Tríade

Disponibilidade é a "propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física, por um órgão ou sistema" (IN01 GSIPR, 2008).

Este pilar ocupa posição de destaque e é comumente o que mais enfrentamos nos problemas no dia-a-dia, afinal, quem nunca teve problemas com um site da internet ou com um caixa eletrônico de banco?

O alto grau de dependência dos sistemas informatizados (ou não) nos leva a inviabilidade de viver um cotidiano padrão, caso algum destes sistemas se torne indisponível. Mas não podemos nos focar tão-somente nos sistemas informatizados.

Rememorando a história, lembre-se que a Biblioteca de Alexandria foi destruída pelo fogo na Idade Média, indisponibilizando boa parte do conhecimento da Humanidade.

Integridade é a "propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental" (IN01 GSIPR, 2008)

A informação deve ser exata e completa, qualquer alteração ou destruição de toda ou parte dela sem a devida legalidade pode ser corrompida. Notamos aqui a questão da destruição, que por vezes se faz necessária, mas mesmo assim deve seguir normas e procedimentos.

Confidencialidade é a propriedade de que a informação não esteja disponível a quem não tem autorização nem esteja credenciado. Neste pilar temos alguns verbos de suma importância para a sua concretização, que são: classificar, credenciar e autorizar. É muito difícil, ou até mesmo impossível manter algo confidencial sem que os devidos controles sejam aplicados, surgindo as dúvidas: qual o grau de sigilo desta informação? ou quem poderá manuseá-la?

Outras questões, como a Autenticidade, Controle de Acesso, "Não Repúdio", entre outras, também serão tratadas por este documento, mas são na verdade composições da "Tríade" original, porém de extrema importancia para os orgão públicos.

Autenticidade se refere a certeza de que um objeto provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo. Em telecomunicação, uma mensagem será autêntica se for, de fato, recebida na íntegra, diretamente do emissor. A autenticidade é a garantia de que você é quem diz ser. Em segurança da informação, um dos meios de comprovar a autenticidade é através da biometria, que está ligado diretamente ao **controle de acesso**, que reforça a confidencialidade e é garantida pela **integridade**.

O **Não Repúdio**, visa garantir que o autor não negue ter criado ou assinado o documento.

1.3 Princípios

O conjunto de documentos que compõe esta **POSIC (Política de Segurança da Informação)** deverá se guiar pelos seguintes princípios primários:

- **Simplicidade**: A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos;
- **Privilégio Mínimo**: Usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;
- **Segregação de função**: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos, bem como permitir maior eficácia dos controles de segurança;
- **Auditabilidade**: Todos os eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;
- **Mínima dependência de segredos**: Os controles deverão ser efetivos ainda que se conheça a existências deles e como eles funcionam;
- **Resiliência**: Os controles de segurança projetados para que possam resistir ou se recuperarem dos efeitos de um desastre;
- **Defesa em profundidade**: Os controles de segurança devem ser concebidos em múltiplas camadas de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado.

2. OBJETIVOS

Os objetivos primários da Política de Segurança são :

- Nortear a Administração Municipal Direta e Indireta (referenciada neste documento por *PMJ*) na produção de normas, procedimentos e padrões de Segurança da Informação com o intuito de mitigar falhas nos seus processos de elaboração;

- Criar um arcabouço, onde a PMJ possa organizar estes documentos de forma a serem efetivamente aplicáveis;

- Nortear a PMJ na aquisição de equipamentos e sistemas com padrões de segurança adequados a suas necessidades;

- Nortear a PMJ no desenvolvimento de sistemas informáticos;

- Criar e alterar processos de formação a balancear segurança e agilidade, com foco a minimizar a burocracia, sem prejuízo à segurança;

- Padronizar as exigências de normas de segurança nas contratações de serviços críticos;

- Definir o órgão responsável pela gestão dos incidentes de segurança da informação na PMJ.

Estes objetivos visam a garantir a Segurança da Informação, desde a sua produção até a sua correta destruição.

2.1. Referências Legais e Normativas

Várias Leis Federais e recomendações dos Tribunais de Contas do Estado e da União tratam do assunto. Dentre elas, podemos citar o Código Civil atual, as Leis que tratam do arquivamento de documentos, Lei de Acesso a Informação e o Marco Civil da Internet. A PMJ, como entidade pública deve possuir padrões que sejam aderentes a estas Leis.

2.2. Responsabilidade

A administração e seus servidores são, em primeira instância, responsáveis pela informação e pela observância de todos os pilares da Tríade. Desta forma cabe a ela a padronização desta atividade.

Especificamente sobre cada informação, a responsabilidade durante todo o seu ciclo de vida (do nascimento ao descarte) é de seu proprietário (quem a gerou) e seu custodiante (quem detém a sua guarda).

2.3. Economicidade

Qualquer incidente envolvendo Segurança da Informação causa prejuízos enormes na imagem e nos cofres públicos, haja vista a grande quantidade de tempo e dinheiro necessários para a recuperação do nível anterior ao evento, isto quando for possível referida recuperação.

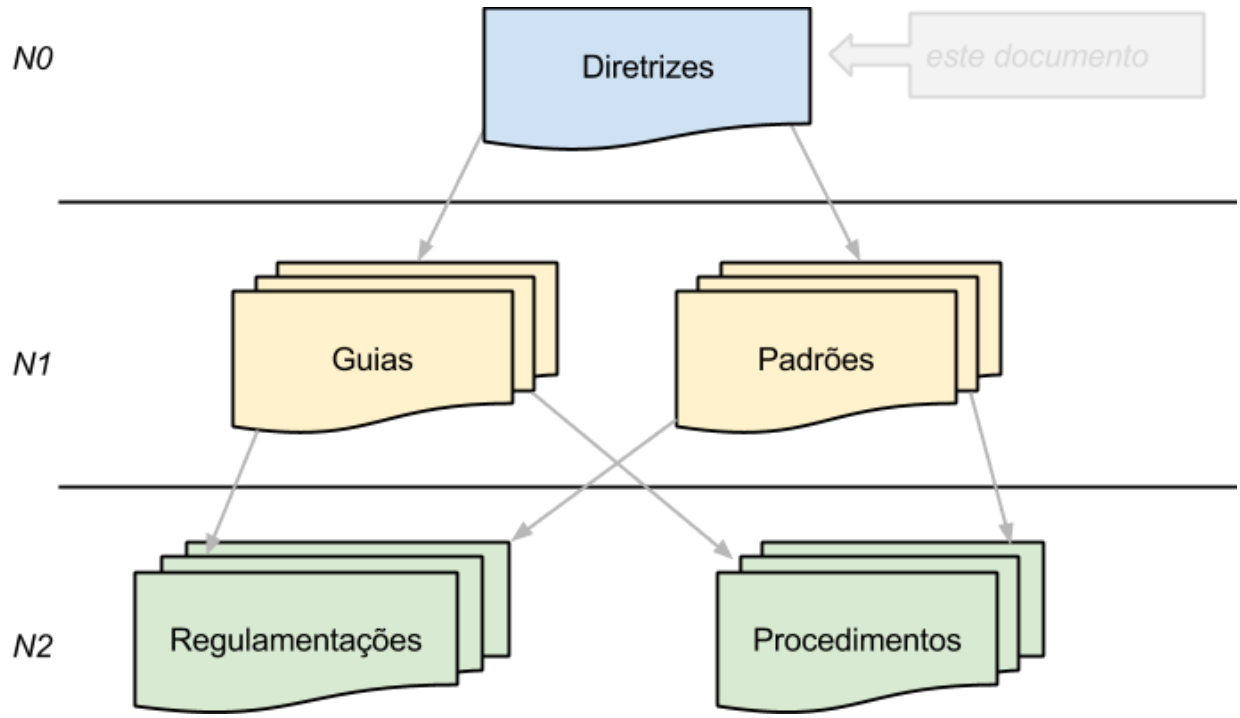
2.4. Comprometimento

Esta Política foi fruto do trabalho conjunto da Administração Pública e dos Servidores Públicos Municipais (representados pelo "Grupo de Segurança"), sendo apresentada e amplamente discutida antes de sua implementação. Assim sendo, existe o compromisso de todos os envolvidos em segui-la e cumpri-la.

3. ESCOPO

Este documento se aplica aos órgãos da Administração Direta e Indireta do Município de Jundiaí, sendo que os documentos indicados como "Padrões", "Guias", "Regulamentações" e "Procedimentos" poderão ter versão específica para cada entidade. Ele criará um arcabouço/infraestrutura onde os outros documentos correlatos se correlacionam.

3.1. Estrutura



Este documento é a Política Institucional - N0, que é a referência para todos os documentos.

Os documentos chamados de Política N1 terão o papel de descrever os itens aqui indicados, podendo ser estes personalizados para cada ente da Administração Indireta, apontando os controles propriamente ditos, nomeados pelo nível N2.

Assim, o Escopo deste documento é criar, descrever e orientar o arcabouço da Política de Segurança da Informação da Prefeitura de Jundiaí.

4. COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO

É o grupo que tem como função primária a manutenção e elaboração das Políticas de Segurança, podendo também ser consultado em caso de incidentes.

4.1. Estrutura

Constituído por 1 (um) representante de cada órgão da Administração Direta e 1 (um) suplente dos mesmos órgãos, sendo estes indicados pelos Secretários/Representantes e endossados pelo Secretário Municipal de Administração e Gestão.

Além destes representantes, fará parte do Comitê, na mesma composição, 1(um) representante e 1 (um) suplente, as seguintes entidades:

1. Companhia de Informática de Jundiaí - CIJun;
2. Instituto de Previdência do Município de Jundiaí - IPREJUN;
3. DAE S/A - Água e Esgoto;
4. Fundação Municipal de Ação Social - FUMAS;
5. Faculdade de Medicina de Jundiaí;
6. Núcleo de Segurança da Informação;
7. Controladoria Geral do Município;
8. Ouvidoria Municipal;
9. Guarda Municipal.

O Secretário/Representante do órgão pode a qualquer momento alterar a indicação. Na primeira reunião, haverá a eleição do Presidente, Vice, Secretário e 2º Secretário, ocorrendo nova eleição com periodicidade anual.

4.2. Responsabilidades

O Comitê Gestor da Segurança da Informação é o órgão consultivo máximo na decisão dos assuntos relacionados à Segurança da Informação (ver tabela de responsabilidades), sendo a sua decisão diretamente enviada ao Prefeito Municipal.

Constituem responsabilidades do Comitê Gestor da Segurança da Informação:

Item	Cria	Altera	Publica	Decreto Executivo
Política N0*	NÃO	SIM	NÃO	SIM
Política N1	SIM	SIM	SIM	NÃO
Política N2	SIM	SIM	SIM	NÃO

* O Grupo de Segurança da Informação cria a Politica Institucional

4.3. Núcleo de Segurança da Informação

O Núcleo de Segurança da Informação (NSI) é um setor dentro da Secretaria Municipal de Desenvolvimento Econômico Ciência e Tecnologia, cuja função, dentre outras, é promover medidas de forma a cumprir a Política de Segurança da Informação, podendo, pelos meios legais:

- Realizar, sugerir e contratar análises de vulnerabilidades
- Realizar, sugerir e contratar análise de impacto nos negócios;
- Realizar, sugerir e contratar classificação da informação;
- Realizar, sugerir e contratar plano de continuidade dos negócios;
- Propor alterações nas Políticas de Segurança existentes e sugerir novas;
- Propor, sugerir e realizar treinamentos sobre Segurança da Informação;
- Realizar auditoria nos órgãos e nas entidades da Administração Pública, envolvidas com a política de segurança da informação, no intuito de aferir o nível de segurança dos respectivos sistemas de informação;
- Estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação;
- Desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;
- Estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse público;
- Gerir o CSIRT (*Computer Security Incident Response Team* - Grupo de Resposta a Incidentes de Segurança) da PMJ;
- Outras atribuições correlatas a Segurança da Informação.

O NSI (Núcleo de Segurança da Informação), ainda será responsável por:

- Suspender, a qualquer tempo, o acesso do usuário ou do sistema às informações ou recursos de tecnologia da informação e comunicação, quando evidenciados riscos à segurança da informação, notificando, de imediato, o responsável pelo usuário/sistema por meio de relatório circunstanciado;
- Dar tratamento e encaminhamento aos incidentes de redes, tomando as medidas necessárias para conter as ameaças, minimizar os impactos e evitar futuras ocorrências, restabelecendo, juntamente com o setor responsável, a integridade, confidencialidade, disponibilidade e autenticidade dos ativos;
- Registrar, classificar e filtrar as notificações de incidentes de segurança;
- Elaborar e executar o plano de resposta aos incidentes de segurança;
- Recolher e preservar as evidências para subsidiar a forense computacional;
- Investigar as causas dos incidentes;

5. DESCRIÇÃO DAS POLÍTICAS

A Política de Segurança da Informação é o conjunto de documentos estruturados e divididos da seguinte forma:

5.1 Política Institucional N0

Trata-se deste documento aqui transcrito, que cria estrutura e propões regras de longo prazo para a criação e manutenção da Política de Segurança da Informação.

5.2 Políticas N1

São documentos descritivos onde se define o objetivo a ser alcançado para cada controle. Este documento estabelece a criação de Políticas N1 para, **pelo menos,** os itens abaixo relacionados:

5.2.1. Gestão de Ativos

Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.

Exemplos de controle: Padrão de uso de Notebooks e HDs externos, procedimento para identificação de ativos e proprietários, procedimento para classificação da informação, norma com tabela de temporariedade.

5.2.2. Segurança em Recursos Humanos

Objetivo: Assegurar que os servidores, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papeis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos.
Exemplos de controle: Documento de comprometimento de conhecimento da Política de Segurança da Informação, procedimento próprio e adequado no caso de desligamento do funcionário, normas de treinamento em TI continuado.

5.2.3. Segurança Física e do Ambiente

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações da organização.
Exemplos de controle: Normas para acesso em áreas críticas como arquivos e “Data Centers”.

5.2.4. Gestão de Operações e Comunicações

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.
Exemplos de controle: Norma de segregação de função na atribuição de acesso a sistemas, procedimento para controle de ligações, padrão mínimo para “Backups”, padrão para controle das redes, procedimento para descarte de mídias.

5.2.5. Controle de Acesso

Objetivo: Controlar o acesso à Informação

Exemplos de controle: Padrão para uso de sistema de diretório, padrão para uso da Internet, norma para criação e troca de senhas, procedimento para liberação de equipamento pessoal (“BYOD”).

5.2.6. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Objetivo: Garantir que a segurança é parte integrante de sistemas de informação
Exemplos de controle: Procedimento para desenvolvimento com foco em segurança, padrão para contratação de Certificado Digital, padrão para uso de “hash” e mecanismos de criptografia.

5.2.7. Gestão de contratos de Serviços Críticos com fornecedores

Objetivo: Assegurar que a empresa contratada possua os requisitos mínimos de segurança, de forma a garantir as informações e serviços prestados a PMJ.
Exemplos de Controle: Norma de requisitos mínimos de segurança na contratação de serviços críticos, norma de exigência de plano de recuperação de desastres para prestação de serviço em sistemas informatizados.

5.2.8. Gestão de Incidentes de Segurança da Informação

Objetivo: Assegurar que fragilidades e eventos de Segurança da Informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.
Exemplos de Controle: Procedimento no caso de “pixação” em site; norma de notificação de incidentes.

5.2.9. Gestão de Continuidade do Negócio

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, além de assegurar a sua retomada em tempo hábil, se for o caso.

Exemplos de controle: Procedimento para enumeração dos processos críticos de negócio, norma para manutenção da gestão de Processos Administrativos de continuidade.

5.2.10. Conformidade

Objetivo: Evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de Segurança da Informação.
Exemplos de controle: Procedimento de auditoria na rede e acessos, normas de privacidade e acesso à informação.

5.2.11. Gestão de Processos Administrativos

Objetivo: Assegurar o trâmite correto do processo administrativo, assegurando sigilo das informações quando indicado sua guarda e destruição.
Exemplos de controle: Norma para implantação de Gerenciamento Eletrônico de Documentos aplicado a processos, padrão para guarda e descarte de processos físicos.

5.3. Políticas N2

São os controles propriamente ditos, documentos ligados à Políticas N1 que descrevem como os objetivos serão atendidos. São de dois tipos:

- Regulamentações: Definem detalhadamente como serão implantadas as Políticas N1 e seus controles.

- Procedimentos: Explicam a forma de fazer o objeto pretendido.

5.4. Prazos

Prazos para implantação, após o decreto, da Política proposta:

Política	**Implantação**	**Revisão**
N0	Imediata	4 anos
N1	6 meses	anual
N2	1 ano	anual

6. PENALIDADES

Ações que violem a POSIC ou quebrem os controles de Segurança da Informação e Comunicações serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Processo disciplinar específico, quando couber, deverá ser instaurado para apurar as ações que constituem a quebra das diretrizes impostas por esta POSIC.

A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação e Comunicações.

O não cumprimento da POSIC, suas normas e regulamentos, por qualquer pessoa ou sistema, acarreta riscos à segurança da informação, cabendo ao Núcleo de Segurança da Informação avaliar a necessidade e instaurar o processo investigativo apropriado.

As faltas listadas abaixo serão tratadas com agravante:

- Uso de mecanismos de “driblagem” dos sistemas de monitoramento utilizados;
- Uso de “White Proxies”;
- Contaminar ou deixar-se contaminar de forma intencional por algum tipo de “Malware”.

As punições serão efetivadas por meio de processo administrativo próprio e tratadas como dano ao patrimônio público, sem prejuízo da responsabilidade civil e criminal.

São exemplos de crimes definidos na legislação:

- Invasão de dispositivo informático (Lei 12.737, Art. 2º - detenção de 3 meses a 1 ano);
- Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Lei 12.73, Art. 3º - detenção de 1 a 3 anos);
- Divulgação de segredo (Lei 9.983, Art. 2º - detenção de 1 a 4 anos);
- Inserção de dados falsos em sistemas de informações (Lei 9.983, Art. 1º - reclusão de 2 a 12 anos);
- Modificação ou alteração não autorizada de sistema de informações (Lei 9.983, Art. 1º - detenção, de 3 meses a 2 anos, + ⅓ se dano para Administração Pública);
- Dano qualificado (inclui destruição de informação) (Lei 5.346 - detenção de 6 meses a 3 anos).

7. COMUNICAÇÃO E TREINAMENTO

A Política de Segurança da Informação terá divulgação ampla aos servidores e munícipes, através de:

- Documento apropriado na admissão e demissão (com termo de aceite);
- Publicação na Intranet e na Internet;
- Treinamentos próprios contratados;
- Outros meios de divulgação.

8. BIBLIOGRAFIA/REFERÊNCIAS LEGAIS

❖ Lei Federal nº 12.737, de 30 de novembro de 2012 - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

❖ Lei Federal nº 12.735, de 30 de novembro de 2012 - Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

❖ Decreto Federal nº 7.724 de 16 de maio de 2012 - Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

❖ Lei Federal nº 12.527, de 18 de novembro de 2011 - Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

❖ Decreto Federal nº 4.553, de 27 de dezembro de 2002 - Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

❖ Lei Distrital nº 4.990, de 12 de dezembro de 2012 – Regula o acesso a informações no Distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art.

216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal no 12.527, de 18 de novembro de 2011, e dá outras providências.

❖ Decreto Distrital nº 33.528, de 10 de fevereiro de 2012 – Dispõe sobre a aprovação de Estratégia Geral de Tecnologia da Informação – EGTI, elaborada pelo Comitê Gestor de Tecnologia da Informação e Comunicação e dá outras providências.

❖ Lei Distrital nº 2.572, de 20 de julho de 2000 - Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática.

❖ ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Esta Norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

❖ ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação.

❖ Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014.