JUCIS.DF

SEGURANÇA
DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO
PoSIC

DIRETORIA DE TECNOLOGIA
INFORMAÇÃO - DTI

É tempo de ação. GDF

Governador do Distrito Federal
Ibaneis Rocha Barros Júnior

Presidente da JUCIS-DF
Walid de Melo Pires Sariedine

Secretário - Geral
Maxmiliam Patriota Carneiro

Diretora de Tecnologia da Informação
Mariza Avalone Araújo

Equipe de Elaboração
Diretora de Tecnologia da Informação - Mariza Avalone Araújo
Gerente de Soluções Sistêmicas – Larissa Corado Lustosa
Gerente de Infraestrutura Tecnológica – André Rodrigues de Souza Junior
Assessor – Rodrigo Damasceno Santos

Aprovação
Comitê Gestor de Tecnologia da Informação e Comunicação da Junta Comercial, Industrial e Serviços – JUCIS-DF

ÍNDICE

1. Introdução

A Política de Segurança da Informação e Comunicações (POSIC) é um documento que alinhado ao Plano Estratégico da JUCIS-DF visa fornecer diretrizes, critérios e suporte administrativo à implementação da segurança da informação e comunicações.

Este documento tem validade de 04 (quatro) anos, 2022-2026, podendo ser revisado sempre que houver necessidade de alterações que justifiquem mudanças.

No sentido de manter as melhores práticas em segurança da informação, aumentando a governança e gestão nos processos e serviços de SIC (Segurança da Informação e Comunicações), bem como a otimização dos recursos tecnológicos na JUCIS/DF, a POSIC busca garantir a segurança da informação, apresentando os princípios e principais requisitos de segurança da informação.

2. Diretrizes Gerais

São diretrizes gerais da POSIC/JUCIS-DF:

- ✓ A preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem os ativos de informação da JUCIS-DF.
- ✓ Garantia de continuidade das atividades realizadas em meios tecnológicos.
- ✓ Economicidade da proteção dos ativos de informação.
- ✓ Pessoalidade e utilidade do acesso aos ativos de informação.
- ✓ A responsabilização do usuário pelos atos que comprometam a segurança dos sistemas de informação.
- ✓ Documentos corporativos imprescindíveis às atividades dos usuários deverão ser salvos em dispositivos de rede. Os arquivos gravados localmente, nos computadores dos usuários, não serão cobertos pelo serviço de backup (cópias de segurança) estando sujeitos a perda e a não recuperação.

- ✓ Arquivos pessoais e/ou não pertinentes às atividades laborais do servidor (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os dispositivos de rede, pois podem sobrecarregar a capacidade de armazenamento e conter vulnerabilidades e riscos de segurança. Caso identificados, esses arquivos serão excluídos de forma imediata e definitiva sem necessidade de comunicação prévia ao usuário.

3. Objetivos

A Política de Segurança da Informação da Junta Comercial, Industrial e Serviços do Distrito Federal (JUCIS-DF) tem a finalidade de estabelecer diretrizes para a segurança, o manuseio, o tratamento e controle dos dados armazenados ou transmitidos por meios tecnológicos, regular as atividades de tratamento de dados pessoais de pessoas físicas e jurídicas sempre em consonância com as leis estabelecidas, dando aos usuários transparência ao acesso às informações.

A implantação da Política de Segurança da Informação da Junta Comercial, Industrial e Serviços do Distrito Federal (JUCIS-DF) tem o objetivo de:

- ➢ Garantir os direitos individuais e coletivos dos servidores e prestadores de serviço, principalmente a inviolabilidade da sua intimidade e o sigilo das correspondências e das comunicações no âmbito da Junta Comercial, Industrial e Serviços do Distrito Federal.
- ➢ Proteger os dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio tecnológico, no âmbito da Junta Comercial, Industrial e Serviços do Distrito Federal.

4. Abrangência

As diretrizes estabelecidas nesta POSIC/JUCIS-DF aplicam-se a todos os servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que, por força de quaisquer instrumentos, exerçam atividades no âmbito da Junta

Comercial, Industrial e Serviços do Distrito Federal, bem como qualquer pessoa que venha a ter acesso aos ativos de informação da JUCIS-DF.

5. Princípios

Os princípios são os aspectos que determinam o ponto de partida. Normalmente são delimitados por instrumentos legais, diretrizes de governo, recomendações e determinações das instâncias de controle, melhores práticas de mercado e pelo próprio contexto da estrutura de TIC do órgão.

Os princípios que regem a POSIC/JUCIS-DF são os seguintes:

- A garantia do direito à intimidade e ao sigilo da correspondência e das comunicações individuais.
- Todas as informações produzidas ou recebidas pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado do exercício de sua função e/ou atividade profissional contratada pertencem à JUCIS/DF. As exceções devem ser formalizadas entre as partes.
- Todos os ativos de informação da JUCIS/DF, inclusive os recursos de comunicação e computacionais, devem ser utilizados de forma responsável, consciente e aplicados na consecução dos objetivos institucionais.
- Cada usuário é individualmente responsável pela segurança das informações dentro da organização, principalmente daquelas que estejam sob sua guarda ou responsabilidade.
- Quando o objeto for pertinente, deverá constar em todos os contratos/convênios celebrados pelo órgão, cláusula de confidencialidade e de obediência às normas internas de Segurança da Informação e Comunicações a ser observada pelas empresas fornecedoras e por todos os profissionais que vierem a desempenhar atividades profissionais no âmbito dos respectivos contratos, inclusive aqueles firmados junto a organismos internacionais.

- O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

6. Dos conceitos e das definições

Para facilitar a compreensão deste documento foram delimitados alguns conceitos e definições, consideram-se:

- Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização.
- Ativo da Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
- Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
- Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação.
- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
- Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.
- Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.
- Diretriz: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas.

- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
- Gestão de Continuidade de Negócios: Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia a dia.
- Gestão de Riscos: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.
- Gestão de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.
- Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
- Informações Críticas: são as informações de extrema importância para a sobrevivência da instituição.
- Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
- Logon: Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível.

- Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para, em casos de incidentes, garantir a manutenção dos ativos de informação, bem como a continuidade de suas atividades críticas em local alternativo num nível previamente definido.
- Segurança da Informação e Comunicações (SIC): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
- Sistemas de Informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção.
- Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.
- Usuário: servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que exerçam atividades no âmbito da Junta Comercial, Industrial e Serviços do Distrito Federal que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da JUCIS-DF, formalizada por meio da assinatura do Termo de Responsabilidade.
- Vulnerabilidades: conjunto de fatores internos e externos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.
- Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;
- Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à

saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

- Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
- Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

7. Da Segurança da Informação e Comunicação

São normas que visam a garantir segurança às informações e comunicações produzidas no âmbito desta Junta Comercial, Industrial e Serviços do Distrito Federal:

7.1Controle de Acesso

a) O logon e a senha de rede e de sistemas de informações são a identidade do usuário na Junta Comercial, Industrial e Serviços do Distrito Federal.
b) A identidade do usuário é pessoal e intransferível, sendo o usuário o responsável exclusivo pela proteção da sua identidade.
c) Sempre que se ausentar da estação de trabalho, o usuário deve bloquear o acesso, seja por meio do encerramento da sessão virtual, seja por meio do desligamento da máquina.
d) Os dados dos usuários devem estar atualizados no Sistema de Pessoal da JUCIS-DF.
e) O usuário terá acesso apenas aos sistemas e informações que realmente necessitar para a execução de sua atividade laboral.
f) Quando do afastamento, relocação, mudança de responsabilidades ou atribuições dentro da Junta Comercial, Industrial e Serviços do Distrito Federal, devem ser imediatamente revistos os direitos de acesso e uso dos sistemas e informações.
g) Todos os usuários devem preencher e autenticar o termo de responsabilidade ao cadastrar uma senha.

7.2 Senhas

a) Para cadastrar sua senha, o usuário deve digitar no campo (senha) a quantidade de caracteres definido pela Diretoria de Tecnologia da Informação, sem que haja conhecimento de terceiros.
b) Cabe ao gestor de cada área, definir qual(is) o(s) sistema(s) o usuário terá acesso.
c) As senhas devem ser alteradas, pelo menos, uma vez por ano, cabendo ao setor de tecnologia da informação a implementação de meios para promover a alteração.

7.3 Tratamento de Incidentes de Rede

Nos termos da Norma Complementar 05/IN01/DSIC/GSIPR "tratamento de Incidentes de Segurança em Redes Computacionais é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências".

As ocorrências de incidentes de segurança em redes de computadores da JUCIS DF deverão ser comunicadas pela DTI por meio de chamado à SUTIC através do telefone (61) 3342-1740, via Sistema Eletrônico de Informações – SEI e também pelo link: (https://sistemas.df.gov.br/PortalDeServicos/Login).

7.4 Classificação da Informação

As informações sensíveis para a execução dos objetivos, missão e visão da Junta Comercial, Industrial e Serviços do Distrito Federal devem ser classificadas pelo gerador da informação.

7.5 Uso da Internet e Recursos de Tecnologia da Informação

O acesso à Internet no âmbito da Junta Comercial, Industrial e Serviços do Distrito Federal deve ser realizado com a finalidade exclusiva de executar as atividades

de interesse público e àquelas desempenhadas pelo órgão, observando sempre a moralidade administrativa.

São vedados:

a) A instalação de softwares não homologados ou licenciados pelo setor de tecnologia da informação.
b) O acesso ou a tentativa de acesso a recurso tecnológico do qual não seja detentor de autorização, em especial àqueles que contenham conteúdo considerado ofensivo, ilegal ou impróprio.
c) A utilização dos recursos tecnológicos da JUCIS-DF para fins estranhos às atividades desta autarquia.
d) A prática de quaisquer atos tendentes a tornar indisponível qualquer recurso tecnológico sem autorização.
e) O uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente de rede da Junta Comercial, Industrial e Serviços do Distrito Federal.

O usuário é responsável pela integridade do equipamento computacional que está operando.

O Código Penal Brasileiro (Decreto-Lei n° 2848/1940) tipifica como crime o ato de "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (art. 154-A), assim como comete crime "quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (art. 154-B).

7.6 Uso do Correio Eletrônico

a) É obrigatório o uso do correio eletrônico corporativo como meio de envio e recebimento de informações inerentes às atividades institucionais da Junta

Comercial, Industrial e Serviços do Distrito Federal, é vedada a sua utilização para fins particulares.

b) O acesso diário à caixa de mensagens eletrônicas corporativa é responsabilidade exclusiva do usuário.

c) O setor de tecnologia da informação deverá, ouvindo previamente a Presidência do órgão, adotar medidas para bloquear o acesso, pela rede da Junta Comercial, Industrial e Serviços do Distrito Federal, aos correios eletrônicos institucionais dos servidores quando identificado o mau uso.

Os requisitos de segurança da informação devem estar explicitamente citados em todos os termos de compromisso celebrados com terceiros.

Todos os membros, servidores, parceiros, licenciados, fornecedores, terceiros e colaboradores eventuais, usuários dos ativos sigilosos, devem assinar termo de compromisso quanto ao sigilo dos dados, informações e conhecimentos da Junta Comercial, Industrial e Serviços do Distrito Federal.

8. Papéis e responsabilidades em SIC

Tabela com os papéis e responsabilidades estabelecidos em Segurança da Informação e Comunicações (SIC).

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
USUÁRIO INTERNO	Servidores públicos, servidores sem vínculo, demais funcionários e colaboradores internos.	Todos os servidores, gestores, estagiários, terceirizados e demais colaboradores internos, que fazem uso dos recursos informacionais e computacionais da JUCIS-DF.
USUÁRIO EXTERNO	Prestadores de serviço e demais colaboradores externos. Cidadãos que utilizam os serviços digitais da JUCIS-DF.	Prestadores de serviços contratados direta ou indiretamente pela JUCIS-DF e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais. Toda sociedade que utiliza o serviço 100% digital da JUCIS-DF por meio do sistema SRM.
GESTORES	Responsável pelas ações de segurança da informação e comunicações no âmbito do órgão .	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
ÁREA DE TIC	Diretoria de Tecnologia da Informação - DTI	Unidade organizacional responsável pela gestão e operação dos recursos de

		TIC na organização e custodiante da informação.
GESTOR DE SIC	Gerência técnica	Responsável pelas ações de segurança da informação e comunicações no âmbito do órgão.
ETIR	Equipe técnica	Grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores.
SUBCOMITÊ DE SIC	Alta Administração	Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão .

8.1 Responsabilidades gerais

São responsabilidades gerais e comuns a todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação da JUCIS-DF:

a) Zelar pela segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.

b) Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação e comunicação – utilizando-os sempre de forma ética, legal e consciente.

c) Manter-se atualizado em relação a esta POSIC e às suas normas complementares e procedimentos relacionados, buscando informação junto a DTI sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso e/ou descarte de informações.

8.2 Responsabilidades específicas

8.2.1Usuários internos e externos

Os usuários devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos vigentes de segurança da informação e comunicações.

São obrigações do usuário:

- Observar rigorosamente esta Política de Segurança de Informação e Comunicação, bem como as Normas e Procedimentos a ela vinculados;
- Assegurar o uso racional dos recursos de Tecnologia da Informação e Comunicação colocados à sua disposição, priorizando o interesse público e institucional;
- Comunicar a Área competente quaisquer riscos ou incidentes de segurança de que venha a tomar conhecimento;
- Assegurar-se que as senhas e credenciais para acesso aos ativos de processamento e de informações estejam de acordo com os procedimentos estabelecidos e que as mesmas sejam protegidas e confidenciais, não devendo ser compartilhadas, ou seja, toda senha é de uso PESSOAL e INTRANSFERÍVEL;
- Manter, obrigatoriamente, os dados críticos da sua Unidade Administrativa em compartilhamentos de rede disponibilizados pela área de TIC;
- Não utilizar serviços de e-mail gratuitos, como GMAIL, HOTMAIL, UOL e outros, para atividades institucionais, visto que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;
- Ativar e utilizar adequadamente sua conta de e-mail corporativo apenas para fins institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou do próprio Estado, em consonância com as determinações legais;

- Acessar a Internet apenas para navegação em sítios cujo conteúdo esteja adequado aos dispositivos legais, às determinações da Unidade Administrativa e às suas atribuições institucionais.

A JUCIS-DF poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento desta POSIC ou das normas complementares e procedimentos específicos dela decorrentes. O desconhecimento das regras contidas nesta POSIC é inescusável, ou seja, a alegação de seu desconhecimento não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade

8.2.2 Gestores de pessoas e processos

Os gestores executivos da JUCIS-DF devem manter postura exemplar em relação à segurança da informação e comunicações, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de Segurança da Informação e Comunicações, tomando as ações necessárias para cumprir tal responsabilidade.

8.2.3 Diretoria de Tecnologia da Informação – DTI

Quanto à gestão de segurança da informação e comunicações, serão responsabilidades específicas da área de Tecnologia da Informação:

a) Zelar pela eficácia dos controles de SIC utilizados e informar aos gestores e demais interessados os riscos residuais.

b) Negociar e acordar com os gestores níveis de serviço relacionados a SIC, incluindo os procedimentos de resposta a incidentes.

c) Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de Segurança da Informação e Comunicações.

d) Gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes; para as trilhas geradas e/ou mantidas em meio eletrônico,

devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências.

e) Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

f) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados a POSIC - Política de Segurança da Informação e Comunicações.

g) Implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

h) Informar previamente o Gestor de SIC sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante.

i) Nas movimentações internas dos ativos de TIC, assegurar-se de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

j) Gerir a capacidade de armazenamento, processamento e transmissão de dados de forma a garantir os níveis de segurança requeridos.

k) Atribuir a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta.

l) Proteger continuamente todos os ativos de informação contra ameaças de segurança, buscando assegurar que novos ativos apenas sejam integrados ao ambiente de produção após cumprirem os requisitos de segurança da informação definidos.

m) Zelar pela não introdução de vulnerabilidades ou fragilidades indesejadas nos ativos de informação ou nos ambientes informacionais da JUCIS-DF durante sua operação ou durante eventos de mudança de ambiente (de desenvolvimento para teste, homologação ou produção.

n) Definir regras para instalação de softwares e hardwares no ambiente corporativo e demais ambientes vinculados, incluindo aqueles dedicados ao uso pelo público externo;

o) Responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos.

p) Garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do órgão, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos.

q) Comunicar a SUTIC (Subsecretaria de Tecnologia da Informação do GDF), responsável pelo ambiente da JUCIS-DF, por meio da Diretoria de Tecnologia de Informação da JUCIS-DF, sempre que houver incidentes ou necessitar de instalação ou adequação de ativos.

8.2.4 Gestor de Segurança da Informação e Comunicações

Em conformidade com o disposto no artigo 7° da IN GSI/PR n° 01/2008 incumbe ao Gestor de Segurança da Informação e Comunicação:

a) Promover cultura de segurança da informação e comunicação no âmbito de suas atribuições dentro da JUCIS-DF.

b) Acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança da informação.

c) Propor recursos necessários às ações de segurança da informação.

d) Coordenar o Subcomitê de Segurança da Informação e Comunicação e a Equipe Técnica de Tratamento de Incidentes em Redes Computacionais (ETIR).

e) Realizar e acompanhar estudos de novas tecnologias no que tange aos aspectos relacionados à segurança da informação.

8.2.5 Equipe de tratamento e resposta a incidentes em redes computacionais

São responsabilidades específicas da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, apoiar a recuperação de sistemas, realizar análise de ataques e intrusões, cooperar com outras equipes e participar em fóruns e redes nacionais e internacionais.

Cabe a ETIR (Equipe de Tratamento e Resposta e Incidentes em Redes Computacionais) as seguintes atribuições:

a) Gerenciar incidentes de segurança em redes computacionais.

b) Investigar e avaliar danos decorrentes de quebras de segurança.

c) Registrar todos os incidentes de segurança em redes de computadores, com a finalidade de assegurar registro histórico das atividades da ETIR.

d) Realizar tratamento da informação de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

8.2.6 Subcomitê de Segurança da Informação e Comunicação

Compete ao Subcomitê de Segurança da Informação e Comunicação da Junta Comercial Industrial e Serviços do Distrito Federal - JUCIS-DF:

a) Assessorar o órgão na implementação das ações de Segurança da Informação.

b) Constituir grupos de trabalho para tratar temas e propor soluções específicas sobre Segurança da Informação e Comunicação.

c) Propor alterações e revisar periodicamente a Política de Segurança da Informação. e Comunicações da JUCIS-DF em conformidade com a legislação existente sobre o tema.

d) Propor, normas complementares e procedimentos internos de Segurança da Informação e Comunicação, em conformidade com a legislação existente sobre o tema.

e) Propor investimentos relacionados à Segurança da Informação e Comunicação.

g) Encaminhar à Presidência da JUCIS-DF casos de descumprimento da Política de Segurança da Informação e Comunicações ou de suas normas e procedimentos complementares, para análise das medidas corretivas aplicáveis e/ou procedimentos administrativos a serem instaurados.

9. Documentos de Referência

Na aplicação e na interpretação das diretrizes estabelecidas nesta POSIC/JUCIS-DF, devem ser observados os seguintes atos normativos, sem prejuízo da aplicação dos atos que venham a ser editados posteriormente:

- I - 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.
- II - 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.
- III - 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.
- IV - Lei Federal nº 13.709/2018 de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural .
- IV - Lei Federal nº 13.709/2018 de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os

direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

- V - Regimento Interno da Junta Comercial, Industrial e Serviços do Distrito Federal - JUCIS-DF.