JUSTIÇA FEDERAL

PODER JUDICIÁRIO
JUSTIÇA FEDERAL DE 1º GRAU DA 5ª REGIÃO
SEÇÃO JUDICIÁRIA DO CEARÁ

**PORTARIA Nº 0197, de 20 de Março de 2017.**
**DIRETOR DO FORO**

APROVA OS NORMATIVOS QUE ESTABELECEM AS DIRETRIZES E REGULAMENTAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E UTILIZAÇÃO DOS ATIVOS DE INFORMÁTICA NO ÂMBITO DA JUSTIÇA FEDERAL DE PRIMEIRO GRAU NO CEARÁ.

**O DOUTOR BRUNO LEONARDO CÂMARA CARRÁ**, Juiz Federal Diretor do Foro, no uso de suas atribuições legais, e

CONSIDERANDO os termos da Resolução nº 6, de 7 de abril de 2008, do Conselho da Justiça Federal - CJF, que dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus;

CONSIDERANDO a necessidade de atualização periódica da regulamentação da Política de Segurança da Informação da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará (SJCE) de forma a minimizar os riscos à segurança das informações corporativas;

RESOLVE:

Art. 1º - Aprovar os normativos elaborados pela Comissão Local de Segurança da Informação (CLSI) estabelecendo as diretrizes e regulamentações referentes à Política de Segurança da Informação e utilização dos ativos de informática no âmbito da Justiça Federal de Primeiro no Ceará.

Parágrafo único: Integram esta Portaria os seguintes documentos:

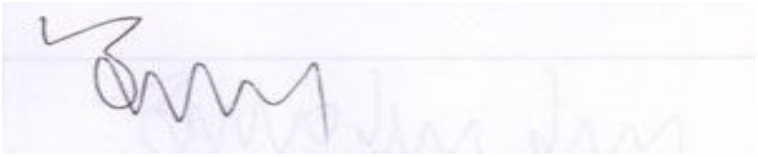
I – Documento de Política de Acesso Físico (ANEXO I) que dispõe de medidas para regular a segurança no acesso físico de pessoas aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI);

II – Documento de Política de Acesso Lógico (ANEXO II), que dispõe de medidas para regular o acesso lógico aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI) da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará (SJCE);

III - Documento de Política de Utilização de recursos (ANEXO III), que dispõe de medidas para regular a utilização dos recursos de Tecnologia da Informação (TI).

Art. 2º Esta portaria entra em vigor a partir de sua publicação.

CIENTIFIQUEM-SE.
PUBLIQUE-SE.
CUMPRA-SE.



BRUNO LEONARDO CAMARA CARRA
JUIZ FEDERAL TITULAR


PODER JUDICIÁRIO
JUSTIÇA FEDERAL DE 1º GRAU DA 5ª REGIÃO
SEÇÃO JUDICIÁRIA DO CEARÁ

# ANEXO I

## Política de Segurança de Acesso Físico

### 1. **Apresentação**

Esta política norteará a implementação de medidas para regular a segurança no acesso físico de pessoas aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI) da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará (SJCE) de forma a minimizarem os riscos à segurança das informações corporativas.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio da instituição, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.2.1 – Política de Segurança de Acesso Físico – do Anexo I da Resolução Nº 6, de 7 de abril de 2008 do Conselho da Justiça Federal que definiu a Política de Segurança da Informação no âmbito do Conselho e da Justiça Federal de primeiro e Segundo graus.

### 2. **Escopo**

O escopo deste documento, integrante da Política de Segurança, da Informação abrange a Justiça Federal de Primeira Instância – Seção Judiciária do Ceará.

3. **Público Alvo**

Esta Política de Controle de Acesso Físico se aplica aos agentes públicos da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas com a administração.

4. **Termos e Definições**

Backup – Cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Fator de Autenticação – Informação que um cliente/usuário sabe (ex: senha), tem (ex.: smartcard) ou é (ex: impressão digital) e é necessária para completar sua autenticação num sistema.

5. **Da Segurança de Acesso Físico**

5.1 Devem ser utilizados perímetros físicos de segurança (barreiras, tais como paredes e portões de entrada controlados) para proteger as áreas que contenham instalações de processamento, armazenamento e comutação de dados, além de controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferências com o suprimento de energia elétrica, interferência nas comunicações, radiação eletromagnética e vandalismo.

5.2 Os perímetros de segurança devem ser claramente definidos e sua localização e a capacidade de resistência dos mesmos devem depender dos requisitos de segurança dos ativos existentes no interior do perímetro.

5.3 A unidade de Tecnologia da Informação (TI) deverá avaliar e providenciar constantemente, com o auxílio das áreas competentes, a melhoria dos recursos de segurança de seus centros de processamento, armazenamento e comutação de dados corporativos.

5.4 As áreas de processamento, armazenamento e comutação de dados devem ser protegidas por controles apropriados de entrada, para assegurar que somente pessoas autorizadas tenham acesso.

5.4.1 Devem ser providos controles de autenticação que utilizem, de preferência, autenticação mínima de dois fatores, para autorizar e validar todos os acessos.

5.4.2 Deve ser mantido, de forma segura, um registro de todos os acessos para fins de auditoria;

5.4.3 A data e hora de entrada e saída de visitantes devem ser registradas, e todos os visitantes devem ser supervisionados, a não ser que o seu acesso tenha sido previamente aprovado.

5.4.4 As permissões de acesso devem ser concedidas somente para finalidades específicas, devendo a pessoa autorizada, receber instruções sobre os requisitos de segurança da área e os procedimentos de emergência.

5.4.5 Os direitos de acesso às áreas seguras devem ser revistos e atualizados em intervalos de tempo regulares, e revogados quando necessário.

5.4.6 Aos terceirizados que realizam serviços de suporte, deve ser concedido acesso restrito às áreas seguras ou às instalações de processamento, armazenamento e comutação da informação sensível somente quando necessário. O acesso deverá ser sempre autorizado e monitorado.

5.5 As áreas de processamento, armazenamento e comutação de dados devem estar localizadas de forma discreta, sem indicação de sua finalidade e sem letreiros evidentes que identifiquem a presença de suas atividades, quando aplicável.

5.6 As listas de funcionários e guias telefônicos internos que identifiquem a localização das instalações de processamento, armazenamento e comutação de dados sensíveis não devem ser de fácil acesso ao público.

5.7 Os equipamentos para contingência e mídias de backup devem ficar a uma distância e local seguros, para que não sejam danificadas por um desastre que afete o local principal.

5.8 Não é permitido, nas localizações dos centros de processamento, armazenamento e comutação de dados, o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado e registrado.

5.9 É proibido o consumo de bebidas, comidas e fumo nas proximidades das instalações de processamento, armazenamento e comutação de dados.

## 6. **Periodicidade de Revisão**

6.1 Esta política deverá ser revista anualmente pelo Comitê Local de Segurança da Informação com vistas a adequa-la às necessidades atuais.

6.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.

## 7. **Penalidades**

9.1 O descumprimento das regras contidas neste documento importará a aplicação das penalidades previstas na legislação vigente, mediante o devido processo legal.


PODER JUDICIÁRIO
JUSTIÇA FEDERAL DE 1º GRAU DA 5ª REGIÃO
SEÇÃO JUDICIÁRIA DO CEARÁ

# ANEXO II

# Política de Controle de Acesso Lógico

## 1. Apresentação

Esta política norteará a implementação de medidas para regular o acesso lógico aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI) da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará (SJCE) de forma a minimizar os riscos à segurança das informações corporativas.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que a informação tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.3.1 – Política de Controle de Acesso Lógico – do Anexo I da Resolução Nº 6, de 7 de abril de 2008, do Conselho da Justiça Federal, que definiu a Política de Segurança da Informação no âmbito do Conselho e da Justiça Federal de Primeiro e Segundo Graus.

## 2. Escopo

O escopo deste documento integrante da Política de Segurança da Informação abrange a Justiça Federal de Primeira Instância – Seção Judiciária do Ceará.

## 3. Público Alvo

A presente Política aplica-se aos agentes públicos da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas.

## 4. Termos e Definições

**Acesso remoto** – Tipo de acesso que possibilita se conectar a um computador e assim controlar e trabalhar diretamente sobre o referido sistema tecnológico, independentemente da distância física.

**Confidencialidade** – Sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-las.

**Criptografia** – Arte e ciência de esconder o significado de uma informação de receptores não desejados.

**Disponibilidade** – Uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

**Fator de Autenticação** – Informação que um cliente/usuário sabe (ex: *senha*), tem (ex.: *smartcard*) ou é (ex: impressão digital) e é necessária para completar sua autenticação num sistema.

**Integridade** – A preservação da integridade envolve proteger as informações contra alterações, intencionais ou acidentais, em seu estado original.

**Log** – Registros de dados que armazenam informações de auditoria.

**OTP** – *One Time Password*. É uma senha que perde a validade após um processo de autenticação. Geralmente uma nova senha é gerada de forma aleatória e em intervalos de tempo regulares.

**Privilégio Mínimo** – Permissão para o usuário acessar apenas os recursos necessários para realizar a sua tarefa.

**Recursos de TI** – Recursos de Tecnologia da Informação. Softwares e hardwares que geram, processam, recebem ou transmitem informações como desktops, notebooks, sistemas operacionais, processadores de texto, *smartphone*, *pendrive*, etc.

**Rede de dados institucional** – Todos os segmentos de rede de dados disponibilizados pela SJCE.

**Rede de dados institucional restrita**– Todos os segmentos de rede de dados onde estão disponibilizados os serviços institucionais restritos aos agentes públicos da SJCE e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas. Todos os equipamentos utilizados nessa rede são de propriedade exclusiva da instituição ou por ela autorizados.

**Rede de dados institucional sem fio** – Todos os segmentos de rede de dados disponibilizados pela SJCE através da tecnologia sem fio.

**Smartcard** - é um cartão que geralmente assemelha-se em forma e tamanho a um cartão de crédito convencional. Muito utilizado para armazenar informações relativas a certificados digitais.

**Smartphone** – Telefone móvel, dotado de grande capacidade computacional, cumprindo funções de telefone celular, agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e redes de computação.

**Usuários** – agentes públicos, estagiários, aprendizes, parceiros e contratados.

**VPN** – *Virtual Private Network*. É uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, implementada em cima de uma rede de comunicações pública (como por exemplo, a Internet).

## 5. Identificação dos usuários

5.1 A gestão de credenciais de identificação de usuários, assim como de seus perfis de acesso aos recursos de rede e sistemas da SJCE, inclusive correio eletrônico, deve ser realizada pela unidade de Tecnologia da Informação (TI) por solicitação formal da autoridade competente.

5.2 O acesso aos recursos de tecnologia da informação somente deve ser permitido aos usuários previamente autorizados mediante identificação.

5.3 As autorizações devem ser definidas de acordo com a necessidade de condução das tarefas institucionais e considerando o princípio de privilégio mínimo.

5.4 Somente usuários que pertençam à unidade de Tecnologia da Informação (TI) poderão possuir privilégio de administrador de computadores/sistemas, ressalvando-se a possibilidade de se delegar tal privilégio em situações específicas e por tempo determinado, apenas e tão somente quando o acesso remoto não se mostrar suficiente para a solução do problema ou a adoção da providência necessária.

5.5 Os usuários da unidade de TI deverão possuir privilégio de administrador de computadores/sistemas apenas se necessário para o cumprimento de suas atividades, obedecido o princípio de privilégio mínimo.

5.6 Sempre que possível, o controle de acesso aos recursos de TI deverá possuir, pelo menos, dois fatores de autenticação.

5.7 As credenciais de identificação do usuário, a exemplo de dispositivos OTP, *login*/senhas e *smartcards*, são únicas, pessoais e intransferíveis, não devendo ser compartilhadas. Sua utilização ou conseqüências decorrentes do seu uso indevido são de responsabilidade do usuário. Nenhum usuário deve identificar-se como outro usuário.

5.8 Não haverá credencial de identificação de usuário genérica e de uso compartilhado para acesso aos recursos de TI, excetuando-se os casos de necessidade justificada. Nestes casos, a unidade de TI deverá ser consultada para emissão de parecer acerca dos riscos associados.

5.9 As senhas dos usuários devem ser escolhidas seguindo critérios a serem definidos pela unidade de TI. Tais critérios deverão considerar, entre outros:

5.9.1 Mecanismos para impedir a geração de senhas fracas ou óbvias;

5.9.2 Conjunto de caracteres permitidos;

5.9.3 Tamanho, vigência, forma de troca e restrições específicas para as senhas;

5.9.4 Segurança da distribuição de senhas (inicial ou não);

5.9.5 Bloqueio ou desativação de usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso malsucedidas.

5.10 Fica assegurado à Comissão Local de Resposta a Incidentes (CLRI), a qualquer tempo, decidir pela suspensão temporária do acesso de usuário ao recurso computacional da SJCE quando evidenciados os riscos à segurança da informação.

5.11 É proibida a utilização de senhas sem nenhum processo criptográfico aplicado, excetuando-se os casos em que não houver alternativa.

**6. Processo de desligamento ou movimentação de usuário**

6.1 Em regra, somente serão concedidas credenciais de acesso aos usuários que estejam em atividade na SJCE.

6.2 As credenciais, identificações, crachás, equipamentos, mecanismos e acessos lógicos devem ser revogados e/ou inutilizados quando do desligamento do usuário.

6.3 A unidade de gestão de pessoas será responsável pelo envio da informação de desligamento ou movimentação de magistrados, servidores, estagiários e aprendizes integrantes da SJCE à unidade de TI para os devidos ajustes das credenciais de acesso.

6.4 O desligamento ou movimentação de usuários não mencionados no item 6.3 deverá ser comunicado à unidade de TI pelo gestor ou responsável pelo respectivo contrato/convênio.

**7. Acesso à rede institucional**

7.1 É vedada a conexão de equipamento, ligado à rede institucional da SJCE, a outros sítios através da utilização de linha discada, rede sem fio, ou quaisquer outros meios, exceto em casos de comprovada necessidade, mediante autorização fundamentada em parecer técnico favorável da unidade de TI.

7.2 É vedada a utilização de microcomputadores ou dispositivos eletrônicos não pertencentes à SJCE, portáteis ou não, na rede institucional restrita, exceto em casos de comprovada necessidade, mediante autorização fundamentada em parecer técnico favorável da unidade de TI.

**8. Acesso remoto à SJCE**

8.1 É proibido o acesso remoto à rede institucional da SJCE por meios que não apliquem criptografia ao tráfego durante o acesso.

8.2 O acesso remoto à rede institucional da SJCE deverá ser precedido de solicitação formal explicitando os motivos de tais necessidades, o período de utilização e os serviços a

serem utilizados. A autorização ficará condicionada a parecer técnico favorável da unidade de TI.

8.3 As conexões de acesso remoto deverão ser precedidas da assinatura do Acordo de Requisitos a Acesso Remoto, documento a ser mantido e atualizado pela unidade de TI.

8.4 O usuário com privilégio de acesso remoto é responsável por garantir que nenhuma outra pessoa, com acesso físico ou lógico ao dispositivo que está efetuando a conexão, viole qualquer política da SJCE, execute atividades ilegais e/ou utilize o acesso para desenvolver atividades pessoais. Este usuário detém a responsabilidade pelas consequências do mau uso do acesso remoto.

8.5 A segurança do acesso remoto deve ser controlada. O controle deverá ser feito através de autenticação forte, de preferência com utilização de autenticação de no mínimo dois fatores e de regras de filtragem que reforcem o princípio do privilégio mínimo.

8.6 As credenciais de acesso remoto são pessoais e intransferíveis, sendo o usuário responsável pela segurança das informações.

8.7 Estações de trabalho ou dispositivos móveis que serão utilizados para o acesso remoto deverão ser disponibilizados preferencialmente pela unidade de TI e ter suas configurações por ela aprovadas.

8.8 As informações de controle dos acessos remotos (*logs*) deverão ser registradas e auditadas periodicamente pela unidade de TI para apuração de eventuais violações de segurança e contabilização do uso de recursos.

## 9. Utilização de sistema de mensageria institucional

9.1 O sistema de correio eletrônico da SJCE não deve ser utilizado para a criação ou distribuição de quaisquer mensagens que não sejam compatíveis com as atribuições dos usuários, incluindo, mas não se limitando a, ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade.

9.2 Cabe à Administração da SJCE, mediante solicitação formal e parecer técnico emitido pela unidade de TI, autorizar a criação de listas de endereços de *e-mail* para

veiculação de assunto dos juízes e servidores, inclusive para temas não compreendidos pelo item 9.1.

9.3 Todos os *e-mails* armazenados, transmitidos ou recebidos pelo sistema de correio eletrônico da SJCE são passíveis de auditoria, podendo ser rastreados por *softwares* específicos para a verificação e adequação às normas estabelecidas na Política de Segurança da Informação do Conselho e Justiça Federal de Primeiro e Segundo Graus e na legislação brasileira.

9.4 O envio de mensagens através de listas de endereços de *e-mail* deve restringir-se a assuntos referentes às suas respectivas temáticas.

9.5 É proibido o envio de *spam* ou mensagens que contenham *software* malicioso por parte dos usuários do sistema de correio eletrônico da SJCE.

9.6 A SJCE deverá prover mecanismos para a identificação de mensagens que possuam conteúdo infectado por *softwares* maliciosos ou que ofereçam risco à segurança da informação. Tais mensagens, quando detectadas, poderão ser excluídas automaticamente ou armazenadas em quarentena.

9.7 Cabe à Administração da SJCE, mediante parecer técnico emitido pela unidade de TI, estipular as regras de utilização do correio eletrônico que se façam necessárias para o bom funcionamento do serviço e à segurança das informações, tais como: quantidade máxima de destinatários, tamanho máximo das caixas postais, tipos e tamanho máximo de arquivos anexos permitidos, periodicidade de leitura obrigatória das mensagens recebidas e criação e exclusão de listas de endereços de *e-mail*.

## 10. Utilização de sistema de mensageria instantânea

10.1 A SJCE proverá sistemas de mensageria instantânea para a comunicação entre os seus usuários e outros órgãos.

10.2 Cabe à Administração da SJCE, mediante parecer técnico emitido pela unidade de TI, definir a solução de mensageria instantânea a ser utilizada pela SJCE.

10.3 A utilização ou conexão com sistemas de mensageria instantânea de uso não institucional deverá ser precedida de solicitação formal à Administração da SJCE, que decidirá mediante parecer técnico da unidade de TI.

10.4 O sistema de mensageria instantânea da SJCE não deve ser utilizado para a criação ou distribuição de quaisquer mensagens que não sejam compatíveis com as atribuições dos usuários, incluindo, mas não se limitando a, ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade.

## 11. Acesso à Internet

11.1 O acesso aos serviços disponibilizados na Internet será provido aos usuários conforme parâmetros estabelecidos pela SJCE, obedecendo ao princípio de privilégio mínimo.

11.2 O acesso a serviços que não se enquadrem na previsão do item anterior deverá ser precedido de solicitação formal à Administração da SJCE, que decidirá mediante parecer técnico da unidade de TI.

11.3 A unidade de TI utilizará *softwares* específicos que efetuarão o registro de todos os acessos aos serviços providos na Internet, assim como o bloqueio dos serviços não autorizados.

## 12. Conexão e Acesso para Terceiros

12.1 Toda conexão de rede de dados entre a SJCE e terceiros que necessitam de acesso remoto, independente da tecnologia de circuito de telecomunicação ou de VPN, deve ser autorizada pela Administração da SJCE mediante solicitação formal e parecer técnico emitido sob a perspectiva de segurança da informação pela unidade de TI. A análise deverá garantir que todos os acessos estejam de acordo com as necessidades do serviço da melhor maneira possível, e que o princípio do privilégio mínimo será seguido.

12.1.2 Toda nova requisição de conexão entre a SJCE e terceiros necessita que seus representantes concordem e assinem o Acordo de Conexão de Remota.

12.1.3 Cabe à Administração da SJCE, mediante parecer técnico emitido pela unidade de TI, estipular as regras para conexão e acesso remoto para terceiros.

## 13. Acesso à rede sem fio

13.1 As exigências que se seguem atingem todos os dispositivos de comunicação de dados conectados à rede institucional sem fio da SJCE.

13.1.1 Todos os pontos de acesso sem fio conectados à rede institucional da SJCE deverão ser submetidos ao controle da unidade de TI. Esses pontos de acesso serão objeto de periódicos testes de penetração e auditoria.

13.1.2 Todas as conexões à rede sem fio deverão ser aprovadas em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

13.1.3 O acesso aos serviços disponibilizados na rede institucional restrita, a partir da rede sem fio, será provido aos usuários conforme parâmetros estabelecidos pela SJCE, obedecendo ao princípio de privilégio mínimo.

## 14. Periodicidade de Revisão

14.1 Esta política deverá ser revista anualmente pelo Comitê Local de Segurança da Informação com vistas a adequá-la às necessidades atuais.

14.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.

## 15. Penalidades

15.1 O descumprimento das regras contidas neste documento importará a aplicação das penalidades previstas na legislação vigente, mediante o devido processo legal.


PODER JUDICIÁRIO
JUSTIÇA FEDERAL DE 1º GRAU DA 5ª REGIÃO
SEÇÃO JUDICIÁRIA DO CEARÁ

# ANEXO III

## Política de Utilização de Recursos de TI

### 1. Apresentação

Esta política norteará a implementação de medidas para regular a utilização dos recursos de Tecnologia da Informação (TI) utilizados pelos usuários da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará (SJCE) de forma a minimizarem os riscos à segurança das informações corporativas.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio da instituição, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.3.2 – Política de Utilização de Recursos de TI – do Anexo I da Resolução Nº 6, de 7 de abril de 2008 do Conselho da Justiça Federal que definiu a Política de Segurança da Informação (PSI) no âmbito do Conselho e da Justiça Federal de Primeiro e Segundo Graus.

### 2. Escopo

O escopo desta Política de Segurança da Informação abrange a Justiça Federal de Primeira Instância – Seção Judiciária do Ceará.

### 3. Público Alvo

Esta Política de Controle de Acesso Lógico se aplica aos agentes públicos da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas com a administração.

## 4. Termos e Definições

**Arquivo** – agrupamento de registros que, geralmente, seguem uma regra estrutural, e que contém informações (dados).

**Backup** – Cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

**Confidencialidade** – sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-las.

**Criptografia** – arte e ciência de esconder o significado de uma informação de receptores não desejados.

**Disponibilidade** – uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

**Hardware** – parte física de um dispositivo eletrônico, sendo formado pelos seus componentes, tais como unidade central de processamento, memória e os dispositivos de entrada e saída.

**Integridade** – a preservação da integridade envolve proteger as informações contra alterações, intencionais ou acidentais, em seu estado original.

**Smartphone** – telefone móvel, dotado de grande capacidade computacional, cumprindo funções de telefone celular, agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e redes de computação.

**Software** – sequência de instruções para serem interpretadas por um computador com o objetivo de executar tarefas específicas.

**Pendrive –** dispositivo portátil de armazenamento com memória *flash*, acessível através da porta USB (*Universal Serial Bus*).

**Privilégio Mínimo** – conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades.

**Programa** – uma coleção de instruções que descrevem uma tarefa a ser realizada por um computador.

**Recursos de TI** – Recursos de Tecnologia da Informação. Softwares e hardwares que geram, processam, recebem ou transmitem informações como desktops, notebooks, sistemas operacionais, processadores de texto, *smartphone*, *pendrive*, etc.

**Rede de dados institucional** – Todos os segmentos de rede de dados disponibilizados pela SJCE.

**Rede de dados institucional restrita**– Todos os segmentos de rede de dados onde estão disponibilizados os serviços institucionais restritos aos agentes públicos da SJCE e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas. Todos os equipamentos utilizados nessa rede são de propriedade exclusiva da instituição ou por ela autorizados.

**Rede de dados institucional sem fio** – Todos os segmentos de rede de dados disponibilizados pela SJCE através da tecnologia sem fio.

**Tablet** – dispositivo pessoal em formato de prancheta que pode ser usado para acesso à Internet, organização pessoal, visualização de fotos, vídeos, leitura de livros, jornais e revistas, entre outros. Apresenta uma tela sensível ao toque que é o dispositivo de entrada principal.

**Usuários** – agentes públicos, estagiários, aprendizes, parceiros e contratados.

## 5. Dos Recursos de TI

5.1 Todos os recursos de TI disponibilizados pela SJCE são de sua propriedade.

5.2 Todas as informações geradas, recebidas, processadas ou armazenadas utilizando os recursos de TI da SJCE são passíveis de auditoria.

5.3 A utilização dos recursos de TI deve ser realizada respeitando-se os princípios da legalidade, moralidade, economicidade e eficiência.

5.4 Os usuários devem ter acesso unicamente àqueles recursos de tecnologia da informação que forem indispensáveis à realização de suas atividades, obedecendo ao princípio do privilégio mínimo.

5.5 Os recursos de TI disponibilizados nas diversas áreas da SJCE destinam-se, exclusivamente, ao atendimento das necessidades do serviço público, sendo vedada sua utilização para fins particulares.

5.6 Os usuários são responsáveis pelos recursos de TI por eles utilizados, devendo contribuir para seu funcionamento e segurança.

5.7 As paralisações programadas de quaisquer serviços disponibilizados pela SJCE devem ser comunicadas com antecedência aos usuários, indicando os períodos de indisponibilidade dos serviços.

5.8 É vedada a utilização de recursos de TI particulares, na rede de dados institucional restrita da SJCE, sem prévia solicitação formal justificando a necessidade de utilização do recurso e autorização da Administração da SJCE, mediante parecer técnico emitido pela unidade de Tecnologia da Informação (TI).

5.9 Os parâmetros de configuração de *hardwares* e *softwares* dos recursos de TI serão definidos pela unidade de TI, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional da SJCE.

5.10 A unidade de TI deverá manter lista atualizada de *hardwares* e *softwares* homologados que poderão ser utilizados no ambiente de TI da SJCE obedecendo ao princípio de privilégio mínimo.

5.11 É vedada a utilização de *hardwares* e *softwares* que não estejam previamente licenciados e homologados.

5.12 A unidade de TI poderá proceder à desinstalação sumária dos softwares e hardwares que estejam em desacordo com os itens 5.10 e 5.11 deste documento.

5.13 A unidade de TI deverá prover mecanismos que proíbam o acesso à rede de dados institucional da SJCE de dispositivos que não estejam em conformidade com os padrões de segurança definidos.

## 6. Das Estações de Trabalho

6.1 As estações de trabalho fornecidas possuirão configurações de *hardware* e *software* padronizadas de acordo com a necessidade de utilização dos usuários.

6.2 Nas estações de trabalho somente devem ser instalados *softwares* homologados e licenciados pela unidade de TI e necessários para execução das atividades dos usuários.

6.3 É vedado ao usuário abrir o gabinete das estações de trabalho e modificar a configuração do *hardware* e/ou *software*.

6.4 O usuário deve informar à unidade de TI quando identificar violação da integridade física do equipamento por ele utilizado.

## 7. Computação Móvel

7.1 Os dispositivos móveis devem ser utilizados obedecendo ao princípio do privilégio mínimo.

7.2 Aplicam-se, quando pertinentes, aos dispositivos móveis, as mesmas regras de utilização das estações de trabalho.

7.3 O NTI deverá prover sistemas que efetuem o bloqueio de utilização de dispositivos móveis, sem autorização, nos recursos de TI, a fim de evitar a fuga de informações confidenciais.

7.4 Os equipamentos portáteis, particulares ou da SJCE, quando não estiverem sendo utilizados, devem ser guardados em local seguro.

7.5 O usuário, ao solicitar o empréstimo de equipamentos portáteis da SJCE, deve fazê-lo ao gestor da área responsável pela guarda do referido dispositivo, tornando formal a solicitação por meio de documento oficial.

7.6 Na devolução do equipamento portátil, o usuário que o utilizou deve retirar todos os arquivos gravados e manipulados, durante sua utilização, além de todos os objetos pessoais, como *pendrives*, cd's, dentre outros.

7.7 Os arquivos armazenados nos equipamentos portáteis devem ser, sempre que possível, protegidos por senhas de acesso e/ou criptografia.

**8. Armazenamento de Dados**

8.1 Todas as informações corporativas devem ser armazenadas nos servidores de dados corporativos da SJCE, observada a temporalidade contida nas normas de gestão documental da Justiça Federal.

8.2 A unidade de TI deverá prover os mecanismos necessários para a proteção das informações armazenadas nos servidores corporativos da SJCE visando ~~a~~ garantir a integridade, disponibilidade e confidencialidade das informações e obedecendo sempre ao princípio do privilégio mínimo.

8.3 A unidade de TI deverá efetuar *backup* periódico dos sistemas e das informações corporativas armazenadas nos servidores da SJCE.

8.4 A unidade de TI não é responsável pela salvaguarda das informações armazenadas nas estações de trabalho e dispositivos móveis.

8.5 É vedado o compartilhamento de pastas nas estações de trabalho dos usuários, salvo solicitação justificada à administração da SJCE. Neste caso, cabe à unidade de TI, proceder à realização do compartilhamento e efetuar as configurações de permissão visando o princípio do privilégio mínimo.

8.6 A unidade de TI deverá prover mecanismos de descarte seguro de informação armazenada em meio digital, de forma a preservar a confidencialidade dos dados da SJCE.

**9. Periodicidade de Revisão**

9.1 Esta política deverá ser revista, anualmente, pelo Comitê Local de Segurança da Informação, com vistas a adequá-la às necessidades atuais.

9.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autoriza o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.

**10. Penalidades**

10.1 O descumprimento das regras contidas neste documento importará a aplicação das penalidades previstas na legislação vigente, mediante o devido processo legal.