ATOS DA PRESIDÊNCIA

INSTRUÇÕES NORMATIVAS

INSTRUÇÃO NORMATIVA TRE-RS P N. 100/2022.

DISPÕE SOBRE A INSTITUIÇÃO DAS DIRETRIZES PARA O USO ACEITÁVEL DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO NO ÂMBITO DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o parágrafo 6º do artigo 37 da Constituição Federal, que dispõe sobre a responsabilidade civil objetiva atribuída aos entes estatais;

CONSIDERANDO a necessidade de adequação à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018);

CONSIDERANDO o disposto na Resolução CNJ n. 396/2021 que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o disposto na Resolução TSE n. 23.644/2021, que institui a Política de Segurança da Informação (PSI) da Justiça Eleitoral;

CONSIDERANDO o disposto na Resolução TRE-RS n. 370/2021, que adota a Política de Segurança da Informação (PSI) da Justiça Eleitoral;

CONSIDERANDO a Portaria TSE n. 444/2021, que institui a norma de termos e definições relativa à Política de Segurança da Informação do TSE;

CONSIDERANDO a Portaria GSI/PR n. 93/2019, que aprova o Glossário de Segurança da Informação;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação, preconizadas pelas normas NBR ISO/IEC 27001:2013 e NBR ISO/IEC 27002:2013, às quais as diretrizes para o uso aceitável dos ativos de informação instituídas nesta norma estão alinhadas;

CONSIDERANDO que as informações são armazenadas e veiculadas por diferentes formas, incluindo os recursos de Tecnologia da Informação, e são essenciais ao desempenho das atribuições no âmbito da Justiça Eleitoral;

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são requisitos fundamentais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio Grande do Sul.

RESOLVE:

Art. 1º Instituir as diretrizes para o uso aceitável dos recursos de Tecnologia da Informação no âmbito do Tribunal, bem como os direitos e as responsabilidades dos usuários e usuárias desses recursos.

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeitos desta norma, entende-se por:

I - acesso remoto: toda conexão estabelecida com a rede do Tribunal Superior Eleitoral (TSE) ou Tribunais Eleitorais originada de um ponto externo, fora das dependências do Tribunal ou de suas unidades administrativas;

II - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
III - *antimalware*: programas informáticos desenvolvidos para prevenir, detectar e eliminar *malware* de dispositivos eletrônicos;
IV - *antispam*: serviço de detecção e análise que tem como objetivo bloquear o recebimento de *spam*;
V - ativos de informação e comunicação: meios de armazenamento, de transmissão e de processamento, bem como os sistemas de informação, as instalações e as pessoas que a elas têm acesso;
VI - autenticação de dois fatores (ou duplo fator de autenticação) (2FA): processo de segurança que exige que os usuários e usuárias forneçam dois meios de identificação antes de acessarem suas conta;
VII - autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
VIII - backup (ou cópia de segurança): conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;
IX - código malicioso (ou *malware)*: programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade de sistema;
X - confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;
XI - credencial (ou conta de acesso): permissão, concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário ou usuária e senha);
XII - diretório compartilhado (ou área compartilhada): espaço de armazenamento e compartilhamento de informações de um grupo de usuários e usuárias específico na rede do Tribunal;
XIII - diretório pessoal (ou área privativa): área reservada para armazenamento e compartilhamento de informações de uma usuária ou um usuário interno, incluindo seu e-mail;
XIV - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;
XV - dispositivo: equipamento dotado de capacidade computacional ou dispositivo removível de memória para armazenamento, entre os quais se incluem, não limitando a estes: *notebooks*, *netbooks*, *smartphones*, roteadores, pontos de acesso, *tablets*, *pendrives*, *USBdrives*, HD externo, e cartões de memória;
XVI - estação de trabalho: conjunto de *harware* e *software* fornecido ao usuário e usuária para que este possa executar suas atribuições;
XVII - geolocalização: recurso tecnológico que permite localizar qualquer objeto ou pessoa, por meio da sua posição geográfica, detectada automaticamente por um sistema de coordenadas;
XVIII - integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;
XIX - princípio do menor privilégio: premissa de fornecer as permissões necessárias e suficientes para que um usuário ou usuária possa realizar suas atividades, por um tempo limitado e com os direitos mínimos necessários para as suas tarefas;

XX - recursos de Tecnologia da Informação (TI): são o conjunto de bens e serviços que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação de dados;
XXI - rede de computadores: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;
XXII - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
XXIII - serviços de comunicação: transmissão ou recepção de dados ou informações por meios confinados, por rádio frequência ou por qualquer outro processo eletrônico ou eletromagnético ou ótico, englobam o correio eletrônico, mensagens instantâneas, listas de e-mail e serviços de videochamada;
XXIV - *site* (ou sítio): conjunto de páginas *web* organizadas e acessíveis a partir de um URL da rede interna (intranet) ou da internet;
XXV - *spam*: prática de envio em massa de e-mails não solicitados;
XXVI - URL: sigla de "*Uniform Resource Locator*", traduzida como "Localizador Uniforme de Recursos", indica o endereço de um recurso de informática disponível em uma rede, seja ela a internet ou a intranet de uma organização;
XXVII - usuário ou usuária: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;
XXVIII - usuário ou usuária externa: servidor ou servidora inativa, pessoa física ou jurídica que tenha acesso, de forma autorizada, à informações produzidas ou custodiadas no âmbito da Justiça Eleitoral;
XXIX - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II
DAS DISPOSIÇÕES GERAIS

Art. 3º Esta norma tem como princípio norteador a garantia da segurança, integridade, confidencialidade, autenticidade e disponibilidade dos ativos de informação e comunicação.
Art. 4º O objetivo deste normativo é estabelecer diretrizes para o uso dos recursos de tecnologia da informação sob a responsabilidade do Tribunal, visando sua preservação, respeitando o princípio norteador definido no art. 3º.
Art. 5º Este normativo se aplica a todos magistrados e magistradas, procuradores e procuradoras eleitorais, servidores e servidoras (efetivos e requisitados), ocupantes de cargo em comissão sem vínculo efetivo, estagiários e estagiárias, prestadores e prestadoras de serviço, colaboradores e colaboradoras, bem como a usuários e usuárias externos que utilizam os ativos de informação deste Tribunal, sendo todos corresponsáveis pela segurança da informação.
Art. 6º Respeitado o disposto na Lei Federal n. 9.609/1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos, convênios e instrumentos congêneres, são de propriedade do Tribunal todos os programas desenvolvidos internamente, para fins institucionais.
Art. 7º Os recursos de TI tratados por esta norma destinam-se exclusivamente à execução das atividades da Justiça Eleitoral ou a elas diretamente correlatas.

§ 1º O acesso aos recursos de TI pode ser restringido a horários, dias específicos, feriados ou geolocalização visando a segurança cibernética deste Órgão.
§ 2º Cabe à Secretaria de Tecnologia da Informação (STI) a identificação e operacionalização das restrições necessárias, previstas no parágrafo anterior deste artigo, com o aval do Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSI).
§ 3º Os recursos de TI são passíveis de monitoramento, podendo ser objetos de auditoria para possíveis diligências.
§ 4º O uso de qualquer desses recursos em desconformidade com as diretrizes desta norma estará sujeito a sanções administrativas e penais, na forma da lei.

CAPÍTULO III

DAS ESTAÇÕES DE TRABALHO

Art. 8º Poderá ser fornecido ao usuário ou usuária estação de trabalho, física ou virtual, de uso individual ou compartilhado, para execução de suas atividades laborais ou a elas diretamente correlatas.
Parágrafo único. O fornecimento da estação de trabalho dependerá de prévia análise de disponibilidade de recursos pela STI.
Art. 9º Compete à STI:
I - decidir sobre a desabilitação de dispositivos de *harware*s e *software*s nativos dos equipamentos;
II - configurar as estações de trabalho para bloqueio automático de tela durante período de inatividade;
III - instalar *software*s homologados e licenciados, conforme a necessidade de cada usuário ou usuária e disponibilidade de licenças, se for o caso.
IV - prover manutenção preventiva e corretiva dos equipamentos;
V - padronizar as estações de trabalho, que deverão possuir os seguintes requisitos de segurança, no mínimo:
a) sistema operacional com suporte ativo para recebimento de atualizações com correções de segurança;
b) *software* anti*malware* instalado, ativado, constantemente atualizado e configurado para verificação em tempo real de mídias removíveis;
c) manutenção de *software*s nas versões mais recentes possíveis;
Parágrafo único. É vedado à STI conceder aos usuários e usuárias privilégios de administrador local nas estações de trabalho, salvo em casos excepcionais, mediante justificativa do titular da unidade, e autorização da Assessoria de Segurança Cibernética.
Art. 10. Compete ao usuário ou usuária:
I - bloquear a estação de trabalho sempre que se ausentar do seu posto de trabalho;
II - zelar pela integridade e conservação dos recursos de TI disponibilizados, responsabilizando-se por eventuais danos que venham a ocorrer pelo seu uso indevido;
III - informar à STI caso seja identificada a violação da integridade dos equipamentos;
IV - solicitar à STI a desinstalação de *software*s que não sejam mais úteis para o desempenho de suas atividades institucionais.
Art. 11. É vedada a manutenção ou alteração das configurações de *harware*s e *software*s das estações de trabalho por pessoal não autorizado pela STI.
Art. 12. É vedado aos usuários e usuárias:
I - instalar, por conta própria, quaisquer tipos de *software* nas estações de trabalho, ficando facultada à STI a verificação, de forma presencial ou remota, e a desinstalação, sem necessidade de comunicação prévia;

II - permitir pessoas estranhas aos quadros da Justiça Eleitoral ter acesso aos equipamentos ou recursos de TI do Tribunal;
III - compartilhar diretórios de arquivos locais na rede, sem anuência da STI.
Art. 13. A intenção de aquisição ou instalação de *software*s, equipamentos ou serviços que necessitem de recursos de TI para o seu funcionamento, deve ser submetida à prévia análise da STI.
Parágrafo único. O parecer da STI levará em consideração os riscos de segurança, a padronização e a compatibilidade com as soluções já implantadas.
CAPÍTULO IV
DA REDE CORPORATIVA
Art. 14. A rede corporativa é de uso restrito aos equipamentos de propriedade do Tribunal.
Parágrafo único. Salvo em casos excepcionais, mediante orientação da STI, será admitido o uso de equipamento pessoal, desde que, atendidos os requisitos mínimos de segurança estabelecidos.
Art. 15. É vedada a conexão de qualquer dispositivo na rede corporativa sem o consentimento prévio da STI.
Parágrafo único. O usuário ou usuária que conectar equipamentos em desobediência ao que trata o *caput* deste artigo, causando dano à rede do Tribunal, poderá ser responsabilizado, na forma da lei.
Art. 16. Cabe exclusivamente à STI, ou à pessoa por ela autorizada, a configuração e manutenção dos equipamentos de rede.
Parágrafo único. Os pontos de rede sem utilização deverão permanecer desativados e somente serão reativados por solicitação feita através do canal de atendimento de requisições de serviços.
Art. 17. A STI poderá disponibilizar pontos de rede sem fio para acesso à rede corporativa, desde que, obedecidos os requisitos mínimos de segurança preconizados pelas melhores práticas.
Art. 18. O acesso à rede corporativa poderá ser interrompido, sem aviso prévio ao usuário ou usuária, por meio de ferramentas de monitoramento quando identificados comportamentos ou programas que possam trazer risco à rede do Tribunal.
CAPÍTULO V
DO ARMAZENAMENTO DE ARQUIVOS
Art. 19. O Tribunal fornecerá diretórios de rede, com capacidade de armazenamento limitada, para salvaguardar os arquivos necessários à execução de atividades de interesse da Justiça Eleitoral ou a elas diretamente correlatas, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.
§ 1º Cada unidade do Tribunal disporá de diretório compartilhado, com acesso restrito aos usuários e usuárias lotados na unidade;
§ 2º As informações corporativas de interesse do Tribunal deverão ser armazenadas no diretório compartilhado.
§ 3º Os dados armazenados nas estações de trabalho, física ou virtual, não estão contemplados pelas garantias mencionadas no caput deste artigo.
§ 4º É vedado o armazenamento de arquivos que não possuam relação com as atividades institucionais do Tribunal nos diretórios de rede.
Art. 20. Os parâmetros para utilização dos diretórios compartilhados serão definidos pela STI e poderão incluir restrições de tamanho máximo e tipos de arquivos permitidos.
Art. 21. A STI não se responsabilizará pela realização de cópias de segurança dos arquivos armazenados localmente na estação de trabalho, física ou virtual.
Parágrafo único. Os arquivos de que tratam o caput deste artigo podem não estar mais disponíveis após manutenção preventiva ou corretiva feita pela STI.

Art. 22. O Tribunal se reserva o direito de inspecionar, sem a necessidade de aviso prévio, arquivos armazenados nos discos locais das estações de trabalho e nos diretórios de armazenamento da rede.

§ 1º Os arquivos de uso pessoal, armazenados nos diretórios de rede, poderão ser excluídos pela STI, sem prévia comunicação ao usuário ou usuária proprietários.

§ 2º Consideram-se arquivos de uso pessoal aqueles que contenham músicas, filmes, fotografias, entre outros, de propriedade particular do usuário ou usuária.

Art. 23. O usuário ou usuária deverá garantir que em sua estação de trabalho não permaneçam armazenados dados pessoais, próprios ou de terceiros.

Parágrafo único. Os dados pessoais devem ser apagados das estações de trabalho e dispositivos de armazenamento após término do tratamento que originou sua coleta, a fim de garantir os requisitos de privacidade previstos na Lei Geral de Proteção de Dados Pessoais.

Art. 24. É vedada a utilização de serviços em nuvem de caráter particular para o processamento ou armazenamento de informações de propriedade da Justiça Eleitoral.

§ 1º Constatada a ocorrência descrita no *caput*, a responsabilidade quanto à segurança, confidencialidade, integridade, disponibilidade e autenticidade de tais informações recairá, com exclusividade, sobre o usuário ou usuária.

§ 2º O incidente de segurança da informação no Tribunal resultante da violação ao disposto neste artigo sujeitará o usuário ou usuária responsável às penalidades cabíveis.

CAPÍTULO VI

DO ACESSO REMOTO

SEÇÃO I

DO ACESSO REMOTO PARA SUPORTE TÉCNICO

Art. 25. O acesso remoto para suporte técnico tem por finalidade melhorar a eficiência dos atendimentos e deverá ser realizado:

I - por *software* de acesso remoto homologado pela STI;

II - por pessoa autorizada pela STI;

III - a partir de estações de trabalho de propriedade do Tribunal.

Parágrafo único. Em situações excepcionais, será admitido o acesso remoto para suporte técnico a partir de computadores de uso pessoal, desde que, respeitados os requisitos de segurança estabelecidos pela STI.

Art. 26. É vedado à pessoa que realizar o acesso remoto para fins de suporte técnico:

I - realizar acesso com finalidade diversa a do *caput* deste artigo;

II - visualizar conteúdo armazenado em estação de trabalho por curiosidade ou má-fé;

III - alterar conteúdo da estação de trabalho do Tribunal sem autorização da STI;

IV - obter cópia de conteúdos, protegidos ou não, sem autorização;

V - copiar *software*s licenciados para o Tribunal ou licença de uso deles sem autorização da STI;

VI - interromper intencionalmente o funcionamento de serviço ou sistema;

VII - qualquer ação que comprometa a segurança da rede de computadores da Justiça Eleitoral, da estação de trabalho acessada ou das informações nelas disponíveis.

SEÇÃO II

DO ACESSO REMOTO À REDE CORPORATIVA

Art. 27. Os usuários e usuárias, mediante solicitação justificada da chefia imediata, feita através do canal de atendimento de requisições de serviços, poderão acessar remotamente a rede corporativa do Tribunal.

§ 1º Na solicitação para acesso remoto, deverão ser informados todos os serviços necessários para o desenvolvimento do trabalho do usuário ou usuária.

§ 2º As permissões concedidas para o acesso remoto deverão atender ao princípio do menor privilégio.
§ 3º O acesso remoto deverá exigir autenticação de dois fatores.
Art. 28. O acesso remoto à rede corporativa dar-se-á por estações de trabalho fornecidas pelo Tribunal, mediante disponibilidade, observadas as especificações técnicas definidas pela STI.
§ 1º Computadores particulares não poderão fazer acesso remoto à rede corporativa do Tribunal, salvo em casos excepcionais, mediante a orientação e anuência da STI e condicionado ao atendimento dos requisitos de segurança estabelecidos.
§ 2º No caso de anuência da STI para uso de dispositivo particular para acesso remoto à rede do Tribunal, não será prestado suporte técnico para problemas de *harware* ou *software*s do equipamento.
Art. 29. O extravio da estação de trabalho ou do dispositivo de uso particular autorizado para acesso remoto deverá ser imediatamente comunicado à STI, pelo usuário ou usuária, para revogação das permissões.
Parágrafo único. No caso de omissão que acarrete danos aos recursos de TI do Tribunal, o usuário ou usuária poderá ser responsabilizado ou responsabilizada, após apurações pelas unidades competentes do Órgão.
Art. 30. É vedado o acesso remoto à rede do Tribunal:
I - a partir de computadores de uso público;
II - por meio de redes sem fio não seguras;
III - por aplicativo de acesso remoto não homologado pela STI.
Art. 31. O suporte técnico para o acesso remoto à rede corporativa do Tribunal estará disponível durante o horário de expediente.
Art. 32. O usuário ou usuária, quando utilizar o acesso remoto, deverá permanecer conectado apenas enquanto estiver efetivamente utilizando os serviços que dele necessitem, devendo desconectar-se nas interrupções e no término do trabalho.
Art. 33. O acesso remoto poderá ser interrompido a qualquer momento, independente de comunicação ao usuário ou usuária, na hipótese de ser identificada situação de grave ameaça ou alto risco à integridade da rede interna e dos serviços disponíveis.
Parágrafo único. Em período eleitoral, o acesso remoto à rede corporativa do Tribunal poderá ser interrompido pela STI como ação de prevenção contra eventuais ataques à rede da Justiça Eleitoral.
SEÇÃO III
DOS RECURSOS DE TI PUBLICADOS NA INTERNET
Art. 34. A STI disponibilizará aplicações e serviços na internet, conforme regras específicas e características técnicas de cada serviço.
Parágrafo único. As aplicações e serviços do Tribunal que forem disponibilizados na internet deverão exigir autenticação de dois fatores, exceto quando houver impedimento de ordem técnica.
Art. 35. O Tribunal não se responsabilizará pela infraestrutura tecnológica de terceiros necessária ao acesso a recursos de TI publicados na internet.
CAPÍTULO VII
DOS SERVIÇOS DE COMUNICAÇÃO
Art. 36. Os serviços de comunicação são disponibilizados como ferramenta para comunicação e colaboração, tanto internamente, com o corpo funcional, quanto com o público externo.
Art. 37. Os usuários e usuárias devem reportar o recebimento de mensagens consideradas suspeitas ao serviço de suporte da STI.

Art. 38. O correio eletrônico registrará dados relacionados ao envio e recebimento de mensagens, armazenando dados de remetente, destinatário e assunto para o caso de necessidade de identificação.

Art. 39. O uso do correio eletrônico será monitorado por meio de ferramentas *antispam* com o intuito de minimizar o recebimento de mensagens maliciosas que coloquem em risco a segurança da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio.

Art. 40. A STI poderá implementar mecanismos para coibir o uso indevido dos serviços de comunicação.

CAPÍTULO VIII

DO ACESSO À INTERNET

Art. 41. Será liberado na rede corporativa, independentemente de solicitação, o acesso à internet.

Parágrafo único. Serão bloqueados para todos os usuários e usuárias e em todos os meios de acesso, os *sites* ou serviços reconhecidamente maliciosos, que possam comprometer a segurança da informação ou degradar os *links* de internet do Tribunal.

Art. 42. Poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja nos períodos críticos do calendário eleitoral ou em situações de contingência, tais como:

I - bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios eletrônicos e serviços; e

II - limitação de banda de tráfego de dados.

Art. 43. O acesso do usuário ou usuária poderá ser bloqueado imediatamente em caso de uso indevido dos recursos ou sempre que colocar em risco a segurança da informação na rede de computadores da Justiça Eleitoral.

Art. 44. O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados e configurados pela STI.

§ 1º É proibido o uso de programas ou tecnologias que burlem as restrições administrativas dos sistemas de segurança.

§ 2º O acesso à internet através da rede local cabeada deve ser realizado exclusivamente através da infraestrutura disponibilizada pela STI, sendo vedado o uso concomitante com outras redes eventualmente disponíveis, adaptadores 3G, 4G ou 5G.

CAPÍTULO IX

DOS MEIOS DE IMPRESSÃO

Art. 45. Os recursos de impressão pertencentes a este Tribunal, disponíveis para o usuário e usuária, serão utilizados em atividades estritamente relacionadas às suas funções institucionais.

Art. 46. Os meios de impressão, sempre que possível, devem ser compartilhados por mais de uma unidade, visando a economicidade dos recursos e as recomendações de sustentabilidade.

Parágrafo único. Sempre que possível, deve-se optar pelo compartilhamento digital de documentos.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 47. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvido o Comitê de Segurança da Informação e Proteção de Dados Pessoais.

Art. 48. Esta Instrução Normativa entrará em vigor na data de sua publicação.

DESEMBARGADOR FRANCISCO JOSÉ MOESCH,

PRESIDENTE.

ATOS DA SECRETARIA