MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS

PORTARIA Nº 194 DG, DE 04 DE JULHO DE 2025

Ministério da Integração e do Desenvolvimento Regional - MDR
Departamento Nacional de Obras Contra as Secas – DNOCS
Comitê de Governança Digital - CGD

Institui a Política de Segurança da Informação do Departamento Nacional de Obras Contra as Secas – DNOCS.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS – DNOCS, no uso das atribuições legais que lhe confere o disposto no Art. 68 e respectivo inciso XII da Portaria DNOCS/DG/GAB nº 43, de 31 de janeiro de 2017, em atendimento à Estratégia Federal de Governo Digital e à Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

R E S O L V E:

Art. 1º Aprovar a Política de Segurança da Informação - PSI do Departamento Nacional de Obras Contra as Secas – DNOCS, na forma do Anexo I desta Portaria, de observância obrigatória no âmbito dessa Autarquia Federal.

Art. 2º Revogar:

I - A Portaria nº 319/DG/CRH, de 06 de setembro de 2011, a Política de Segurança da Informação e Comunicações - PoSIC anterior;

II - A Resolução nº 03/DG/CPGE, de 12 de junho de 2012, a Norma Complementar nº 01 à PoSIC anterior.

Art. 3º Esta Portaria entra em vigor em 29 de Agosto de 2025

Fernando Marcondes de Araújo Leão
Diretor-Geral do DNOCS

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I - DOS PRINCÍPIOS GERAIS

Art. 1º. Fica instituída a Política de Segurança da Informação do DNOCS, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º. Esta Política de Segurança da Informação aplica-se a todas as unidades organizacionais do DNOCS, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade deste DNOCS.

CAPÍTULO II - Disposições Gerais

Art. 3º. São objetivos da Política de Segurança da Informação:

I. estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II. estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III. estabelecer competências e responsabilidades quanto à segurança da informação;

IV. nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V. promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional do DNOCS;

VI. fomentar o uso ético, responsável e seguro dos recursos de tecnologia da informação por todos os usuários;

VII. garantir a rastreabilidade das ações realizadas nos ativos de informação institucionais;

VIII. assegurar que contratos e convênios contemplem cláusulas de proteção e sigilo da informação tratada;

IX. padronizar ações preventivas, corretivas e educativas no enfrentamento a incidentes de segurança da informação e privacidade.

Art. 4º. Para os efeitos desta Portaria e de suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO III - Dos Princípios e Diretrizes

Art. 5º. As ações de segurança da informação do DNOCS são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I. disponibilidade, integridade, confidencialidade e autenticidade das informações;

II. continuidade dos processos e serviços essenciais para o funcionamento do DNOCS;

III. economicidade da proteção dos ativos de informação;

IV. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V. observância da publicidade como preceito geral e do sigilo como exceção;

VI. responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII. alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do DNOCS, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

VIII. conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

IX. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação;

X. obediência ao princípio do menor privilégio no acesso aos recursos informacionais;

XI. responsabilização dos usuários por condutas incompatíveis com o ambiente institucional ou violação das normas de segurança;

XII. proteção da informação durante todo o seu ciclo de vida, da criação ao descarte seguro.

Art. 6º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito deste DNOCS e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º. As normas, procedimentos, manuais e metodologias de segurança da informação do DNOCS devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º. As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do DNOCS;

II. ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do DNOCS;

III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

IV. visar à prevenção da ocorrência de incidentes;

V. incluir ações específicas para o uso adequado de recursos como e-mail, mídias removíveis, redes sociais, Internet e serviços em nuvem;

VI. promover o registro e controle de mudanças em ativos tecnológicos que possam afetar a segurança institucional;

VII. garantir salvaguardas contra código malicioso e softwares não autorizados;

VIII. estabelecer padrões mínimos para senhas, autenticação forte e segregação de funções.

Art. 9º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao DNOCS.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no DNOCS compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional do DNOCS, são passíveis de monitoramento e auditoria pelo DNOCS, respeitados os limites legais.

Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do DNOCS a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação do DNOCS.

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do DNOCS, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 13. Todos os contratos de prestação de serviços firmados pelo DNOCS conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como se suas normas decorrentes.

CAPÍTULO IV - Da Gestão de Segurança da Informação

Art. 14. A estrutura de Gestão de Segurança da Informação é composta por:

I. Alta Administração;

II. Comitê de Governança Digital;

III. Gestor de Segurança da Informação;

IV. Gestor de Tecnologia da Informação e Comunicação;

V. Encarregado pelo Tratamento de Dados Pessoais;

VI. Responsável pela Unidade de Controle Interno;

VII. Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e

VIII. Usuários de Informação.

Art. 15. Compete à Alta Administração:

I. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do DNOCS, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e

II. formalizar e aprovar a Política de Segurança da Informação do DNOCS, bem como suas alterações e atualizações.

Art. 16. Compete ao Comitê de Governança Digital:

I. assessorar na implementação das ações de segurança da informação;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V. deliberar sobre normas internas de segurança da informação;

VI. avaliar as ações propostas pelo gestor de segurança da informação.

Parágrafo único. A composição, estrutura, recursos e funcionamento do Comitê de Governança Digital estão definidos em ato administrativo próprio emitido pelo DNOCS, de acordo com a legislação vigente.

Art. 17. Compete ao Gestor de Segurança da Informação:

I. coordenar o Comitê de Governança Digital;

II. coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III. assessorar a Alta Administração na implementação da Política de Segurança da Informação;

IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V. promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII. propor recursos necessários às ações de segurança da informação;

VIII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

XI. manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;

XII. orientar os gestores sobre controles físicos, lógicos e organizacionais aplicáveis à sua unidade;

XIII. definir, em conjunto com a equipe técnica, os critérios para o uso aceitável da tecnologia da informação;

XIV. propor critérios de monitoramento contínuo e auditoria preventiva sobre os ativos e ambientes críticos.

Parágrafo único. O Gestor de Segurança da Informação do DNOCS será designado em ato administrativo próprio, de acordo com a legislação vigente.

Art. 18. Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de

abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 19. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Art. 20. Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 21. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I. facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no DNOCS;

II. monitorar as redes computacionais;

III. detectar e analisar ataques e intrusões;

IV. tratar incidentes de segurança da informação;

V. identificar vulnerabilidades e artefatos maliciosos;

VI. recuperar sistemas de informação;

VII. promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em ato administrativo próprio emitido pelo DNOCS, de acordo com a legislação vigente.

Art. 22. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação do DNOCS.

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 23. A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 24. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I. tratamento da informação;

II. segurança física e do ambiente;

III. gestão de incidentes em segurança da informação;

IV. gestão de ativos;

V. gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI. controles de acesso;

VII. gestão de riscos;

VIII. gestão de continuidade;

IX. auditoria e conformidade.

§ 1º Comitê de Governança Digital poderá definir outros processos de Gestão de Segurança

da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

Art. 25. As políticas, normas, procedimentos, orientações ou manuais de que trata o §2º do art. 16 devem abordar, no mínimo, aspectos relacionados:

I. a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

II. a classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III. a proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV. ao uso aceitável da informação e a utilização de mídias de armazenamento;

V. a entrada e saída de ativos de informação das instalações da organização;

VI. aos perímetros de segurança da organização;

VII. aos controles de acesso baseados no princípio do menor privilégio;

VIII. as etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente;

IX. aos critérios para a comunicação de incidentes aos titulares de dados pessoas e a ANPD;

X. ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

XI. a Política de Gestão de Ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para o a organização; a manutenção de inventario atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

XII. a utilização adequada dos recursos operacionais e de comunicações fornecidos pelo DNOCS, a serem utilizados para fins profissionais, relacionados às atividades do DNOCS, em conformidade com os princípios éticos e profissionais do DNOCS, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação do DNOCS;

XIII. aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV. o acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV. o uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;

XVI. as políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVII. as políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor

privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação do DNOCS;

XVIII. as políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente do DNOCS, dos seus ativos de informação e das ameaças à segurança da informação; a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XIX. as políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que o DNOCS possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX. as políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças;

XXI. as políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações;

XXII. segurança no uso de mídias removíveis, orientando o bloqueio de mídias não autorizadas, e controle de entrada e saída de dados;

XXIII. diretrizes para o uso adequado do e-mail institucional, incluindo proibição de spam, uso pessoal ou difusão de informações sensíveis sem criptografia ou autorização;

XXIV. critérios para o acesso, armazenamento e descarte seguro de documentos físicos e digitais;

XXV. controle do uso da Internet institucional, vedando downloads não autorizados, streaming e navegação em sites inadequados;

XXVI. regras para uso ético de mídias sociais, incluindo a proibição de manifestação institucional sem autorização formal ou divulgação de conteúdo interno.

§ 1º As unidades organizacionais do DNOCS devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações, realizadas pelas unidades do DNOCS, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos no DNOCS devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes

CAPÍTULO V - Das Vedações e Disposições Finais

Art. 26. É vedada a utilização dos recursos de tecnologia da informação disponibilizados

pelo DNOCS para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 27. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pelo DNOCS.

Art. 28. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 29. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Parágrafo único. É dever do usuário comunicar imediatamente quaisquer falhas de segurança, tentativas de acesso indevido, comportamento suspeito ou indícios de contaminação por software malicioso, preservando as evidências, quando possível.

Art. 30. A unidades organizacionais do DNOCS devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 31. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais:

I. Obrigatória e imediatamente aos canais oficiais de atendimento a Serviços de TIC, para o tratamento adequado para solução do incidente de segurança da informação pela ETIR;

II. Opcionalmente à unidade do CGD no SEI, caso necessário informar ao Gestor de Segurança da Informação.

Art. 32. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pelo DNOCS periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 33. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 34. Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente do DNOCS, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 35. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidas ao Comitê de Governança Digital.

ANEXO II

Não conformidade

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Processo Administrativo disciplinar de acordo com a legislação aplicável
2. Exoneração.
3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.
4. Rescisão contratual ao bem do serviço público.

ANEXO III

Concordância

Li e entendi a Política de Segurança da Informação do DNOCS . Entendo que caso venha a violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do DNOCS .

_____

Nome do Servidor/Empregado

_____

Assinatura do Servidor/Data