PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

Documento nº 9520132/2025/GERSOL-PORTOSRIO/SUPTIN-PORTOSRIO/DIRAFI-PORTOSRIO

Rio de Janeiro, na data da assinatura.

Processo nº 50905.001042/2022-66

Interessado: Companhia Docas do Rio de Janeiro - CDRJ (Portos Rio - Autoridade Portuária)

1. INTRODUÇÃO

1.1. A segurança da informação é de suma importância para as instituições públicas brasileiras, garantindo a proteção dos dados sensíveis e o bom funcionamento dos sistemas em um ambiente cada vez mais digital.

1.2. Diante de um cenário cada vez mais complexo e dinâmico das ameaças cibernéticas, é essencial definir políticas e diretrizes claras para garantir a segurança dos sistemas e informações institucionais.

1.3. O presente documento estabelece os princípios, diretrizes e procedimentos que devem ser seguidos por todos os colaboradores, contratados e parceiros desta Autoridade Portuária, em conformidade com a legislação vigente e as melhores práticas de segurança da informação.

1.4. Ao adotar uma abordagem abrangente e proativa para a segurança da informação, buscamos assegurar a confidencialidade, integridade e disponibilidade das informações, promovendo a transparência, eficiência e confiabilidade dos serviços prestados à comunidade portuária.

2. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO - POSIC

2.1. Estabelecer e difundir normas, diretrizes e procedimentos que viabilizem o acesso seguro às informações corporativas de modo que não impeçam e/ou dificultem o processo do negócio, mas garantam os aspectos de integridade, confidencialidade e disponibilidade dos dados e informações sob responsabilidade da PortosRio e a participação e cumprimento de todos os colaboradores nesse processo.

3. ABRANGÊNCIA

3.1. Esta Política e seus anexos aplicam-se a todas as informações em que a PortosRio seja o agente de tratamento, incluindo seus usuários, o meio utilizado para este tratamento - seja digital ou físico - e as dependências físicas que abrigam os ativos críticos de informação. Especificamente, inclui:

3.1.1. Todos os funcionários, estagiários e jovens aprendizes contratados pela PortosRio;

3.1.2. Todos os prestadores de serviço contratados que, em função da sua atividade, necessitem de acesso aos recursos de TIC da PortosRio;

3.1.3. Todos os servidores e agentes públicos de entidades fiscalizadoras que, em função de sua atividade, necessitem de acesso à rede corporativa e aos sistemas de informação da PortosRio;

3.1.4. Todas as instalações destinadas à transmissão e ao processamento de dados sob a responsabilidade da PortosRio, incluindo seus ativos de informação.

4. REFERÊNCIAS LEGAIS E NORMATIVAS

4.1. A presente Política de Segurança da Informação fundamenta-se nas seguintes referências legais e normativas:

4.1.1. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação no âmbito da Administração Pública Federal;

4.1.2. Lei Nº 13.709, de 14 de agosto 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

4.1.3. Portaria nº 93 GSI/PR, de 18 de outubro de 2021, que Aprova o Glossário de Segurança da Informação;

4.1.4. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

4.1.5. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

4.1.6. Norma Complementar nº 05/IN01/DSIC/GSIPR, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal; e

4.1.7. Norma ABNT NBR ISO/IEC 27001:2013, que normatiza o Sistema de Gestão da Segurança da Informação.

4.1.8. Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.

4.1.9. Lei nº 12.527, de 18 de novembro de 2011, que regulamenta o art. 5°, XXXIII, art. 37, §3°, II e art. 216, §2° da Constituição Federal de 1988.

5. CONCEITOS E DEFINIÇÕES

5.1. No âmbito desta POSIC, considera-se:

5.1.1. **Acesso**: Ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

5.1.2. **Administrador de rede**: Indivíduo que administra o segmento de rede correspondente à área de abrangência da respectiva unidade.

5.1.3. **Ameaça:** Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

5.1.4. **Ativos de Informação**: Qualquer recurso que contém ou processa informações. Esses ativos podem ser físicos (Computadores, laptops, servidores, discos rígidos, etc.), digitais (softwares, bancos de dados, e-mails, arquivos de imagem, etc.) ou até mesmo humanos (conhecimento de funcionários, habilidades, experiência, etc.).

5.1.5. **Autenticação:** Processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema.

5.1.6. **Autenticação multifator:** Utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito).

5.1.7. **Autenticidade**: Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou

entidade.

5.1.8. **Backup ou Cópia de Segurança**: Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

5.1.9. **Banco de dados:** Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

5.1.10. **Biometria:** Verificação da identidade de um indivíduo por meio de uma característica física.

5.1.11. **Bloqueio:** Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

5.1.12. **Certificado Digital:** Conjunto de dados de computador, gerados por uma autoridade certificadora, em observância à recomendação internacional ITU-T X.509 que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação.

5.1.13. **Computação em nuvem:** Modelo computacional que permite acesso, por demanda e independente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

5.1.14. **Confidencialidade**: Propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados.

5.1.15. **Conta de serviço:** Conta de acesso à rede corporativa de computadores criada para a realização de um procedimento automático (aplicação, script etc.), sem qualquer intervenção humana no seu uso

5.1.16. **Conta de usuário**: Conta de acesso individual criada em um sistema informatizado que permite a um usuário acessar e utilizar os recursos e serviços oferecidos de forma privativa, protegendo suas informações do acesso não autorizado.

5.1.17. **Continuidade de Negócios:** Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido.

5.1.18. **Controle de Acesso físico:** Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso a locais específicos.

5.1.19. **Controles de acesso lógico:** Conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizado feitas por pessoas ou outros programas de computador.

5.1.20. **Credencial de acesso:** Processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso, em função de autorização prévia e da necessidade de conhecer.

5.1.21. **Crime cibernético:** Ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores, utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro.

5.1.22. **Dado pessoal:** Informação relacionada à pessoa natural identificada ou identificável.

5.1.23. **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.

5.1.24. **Direito de acesso**: Privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo.

5.1.25. **Diretório ou pasta:** Subdivisão lógica de um sistema de arquivos, que permite o agrupamento de arquivos que se relacionam de alguma forma.

5.1.26. **Disponibilidade**: Propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

5.1.27. **Engenharia social:** Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes.

5.1.28. **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR):** Grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Na PortosRio, a equipe foi instituída pela Portaria CDRJ nº 266/2022.

5.1.29. **Firewall**: Dispositivo de segurança para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados.

5.1.30. **Hardware**: Envolve toda infraestrutura física de tecnologia de uma organização, oferecendo todo o suporte em armazenamento, processamento, nas transações e no uso das informações. São computadores, servidores, dispositivos de armazenamento, roteadores, switches, etc..

5.1.31. **Identidade digital:** Representação unívoca de um indivíduo dentro do espaço cibernético.

5.1.32. **Incidente:** Interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

5.1.33. **Incidente de segurança**: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

5.1.34. Infraestrutura de rede: Refere-se a todos os recursos de uma rede que tornam possível a conectividade, a gestão, as operações comerciais e a comunicação de rede ou Internet

5.1.35. **Integridade**: Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

5.1.36. **Invasão**: Incidente de segurança no qual o ataque foi bem-sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização.

5.1.37. **LDAP (Lightweight Directory Access Protocol):** é um protocolo para serviços de diretório que organiza dados hierarquicamente e possibilita que os usuários de uma rede local ou pública localizem dados sobre organizações, indivíduos e outros recursos, como dispositivos, arquivos e aplicações.

5.1.38. **LOG**: Termo utilizado para descrever o registro de eventos relevantes em um dispositivo ou sistema computacional.

5.1.39. **Logon:** Processo utilizado para acessar uma rede de computadores ou sistema informatizado restrito, realizado através da autenticação ou identificação do utilizador, usando credenciais previamente cadastradas no sistema.

5.1.40. **Logoff:** Processo utilizado para encerrar o acesso a uma rede de computadores ou um sistema informatizado restrito, realizado através da autenticação ou identificação do utilizador, usando credenciais previamente cadastradas no sistema.

5.1.41. **Mídias**: Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, Pen Drives, cartões de memória entre outros.

5.1.42. **Não repúdio**: Propriedade que assegura que nem o emissor nem o receptor de uma informação possam negar o fato, a autoria, a responsabilização.

5.1.43. **Obsolescência tecnológica:** Ciclo de vida do software ou de equipamento, definido pelo fabricante ou causado pelo desenvolvimento de novas tecnologias.

5.1.44. **Perfil de acesso:** Conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

5.1.45. **Política de mesa e tela limpa:** Estratégia de segurança da informação que estabelece medidas para garantir que informações sensíveis ou críticas sejam adequadamente protegidas, especialmente quando não estão em uso pelos usuários.

5.1.46. **Proprietário da Informação**: Pessoa ou setor que produz a informação.

5.1.47. **Rede Corporativa:** Sistema de transmissão de dados que transfere ou compartilha informações entre diversos equipamentos de uma mesma corporação, tais como: computadores, servidores de documentos e arquivos, impressoras, etc. e entre alguns desses equipamentos com o mundo externo.

5.1.48. **Rede Privada Virtual (VPN):** Refere-se à construção de uma rede privada, utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

5.1.49. **Servidores corporativos:** São computadores especializados que fornecem diversos serviços essenciais e recursos compartilhados para suportar as operações de uma organização, como armazenamento de dados, hospedagem de aplicações, comunicação, segurança e gerenciamento de rede.

5.1.50. **Servidor de arquivos**: Ambiente dedicado ao armazenamento de arquivos na rede corporativa.

5.1.51. **Severidade**: Índice ou grau que se refere à medição do impacto de um evento ou incidente de segurança da informação.

5.1.52. **Software**: É todo programa executado em um computador, celular ou dispositivo que permita ao mesmo executar suas funções. Exemplo: sistemas operacionais e aplicativos.

5.1.53. **SPAM**: Tipo de mensagem eletrônica recebida pelo usuário sem que este tenha solicitado ou considere a hipótese de recebê-la. Em geral, essa prática tem finalidade comercial, mas também pode ser um meio para a disseminação de golpes (phishing), boatos, difamação, malwares, etc..

5.1.54. **USB (Universal Serial Bus):** É um padrão de tecnologia que permite a conexão e comunicação ente dispositivos, como teclados, mouses, mídias removíveis, etc..

5.1.55. **Usuário**: Pessoa física ou jurídica, com vínculo oficial com a PortosRio ou em condição autorizada por ela que utiliza algum Recurso de TIC ou alguma informação de sua propriedade ou responsabilidade, em qualquer uma de suas formas. São empregados, terceirizados, colaboradores, consultores, auditores, estagiários e jovens aprendizes que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação.

5.1.56. **Vazamento de dados:** Transmissão não autorizada de dados de dentro de uma

organização para um destino ou recipiente externo.

5.1.57. **Vulnerabilidade:** Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

5.2. Para demais conceitos e denominações relacionados ao tema, consulte o Glossário de Segurança da Informação em https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1

6. PRINCÍPIOS

6.1. As ações e iniciativas relacionadas à Segurança da Informação na PortosRio baseiam-se nos seguintes princípios:

6.1.1. **Autenticidade:** Refere-se à garantia de que a informação foi criada, emitida, modificada ou eliminada por uma pessoa física identificável, sistema, órgão ou entidade determinada.

6.1.2. **Confidencialidade:** Este princípio estipula que as informações somente estarão acessíveis ou reveladas a indivíduos, sistemas, órgãos ou entidades autorizadas e devidamente credenciadas.

6.1.3. **Integridade:** Este princípio assegura que as informações não serão alteradas ou eliminadas de maneira não autorizada ou acidental.

6.1.4. **Disponibilidade:** Este princípio assegura que as informações estarão disponíveis e utilizáveis para aqueles que delas necessitam e possuem autorização para acessá-las.

6.1.5. **Privilégio mínimo:** Este princípio determina que o acesso às informações será restringido apenas ao estritamente necessário para o desempenho das funções pertinentes.

6.1.6. **Equidade:** Este princípio estabelece que as normas e regulamentos de segurança da informação serão observados por todos, sem distinção de cargo ou função.

6.1.7. **Privacidade:** Este princípio indica que informações que possam violar o respeito à intimidade, integridade e honra dos cidadãos não serão divulgadas.

7. DIRETRIZES GERAIS

7.1. São diretrizes gerais desta POSIC:

7.1.1. Estar em conformidade com os objetivos estratégicos, processos, requisitos legais e estrutura organizacional da PortosRio;

7.1.2. Implementar medidas e procedimentos que garantam a disponibilidade, integridade, confidencialidade e autenticidade das informações;

7.1.3. Seguir as melhores práticas e diretrizes de Segurança da Informação e Comunicação recomendadas por entidades e órgãos responsáveis pela definição de padrões.

7.1.4. Prever nos contratos de prestação de serviços firmados com a PortosRio a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo ainda, exigir da entidade Contratada, a assinatura de **Termo de Sigilo e Confidencialidade (9520237).**

8. DO TRATAMENTO DA INFORMAÇÃO

8.1. Qualquer recurso informativo gerado, obtido ou mantido no âmbito da PortosRio deve ser protegido contra ameaças, ataques, incidentes e outras formas de violação à segurança da informação, visando reduzir riscos de perda, adulteração ou acesso indevido.

8.2. Toda informação institucional, se em formato eletrônico, será armazenada nos servidores de arquivos e bancos de dados gerenciados pela área de TIC e, se não eletrônica, será guardada em local que a proteja adequadamente.

8.3. Toda informação institucional em formato eletrônico será respaldada por meio de cópias de segurança gerenciadas pela área de TIC e mantida em local que garanta sua segurança e permita a recuperação em caso de perda da informação original.

8.4. O uso dos recursos de tecnologia da informação oferecidos pela PortosRio para acesso,

armazenamento ou transmissão de material discriminatório, malicioso, antiético ou ilegal é estritamente proibido.

8.5. Os usuários de recursos informatizados da PortosRio deverão adotar a "política de mesa e tela limpa" com o objetivo mitigar os riscos de acesso não autorizado, perda ou comprometimento das informações durante e fora do horário regular de trabalho. São consideradas ações dessa política:

8.5.1. Manter documentos e informações sensíveis guardados em locais seguros, como gavetas trancadas, cofres ou arquivos de segurança, especialmente quando não estiverem sendo utilizados.

8.5.2. Desligar os dispositivos eletrônicos, como computadores e terminais, ou implementar medidas de bloqueio de tela, como senhas ou outros mecanismos de autenticação, quando não estiverem sendo monitorados ou em uso ativo.

8.6. As Unidades Administrativas devem observar as seguintes diretrizes fundamentais ao classificar e tratar informações da PortosRio:

8.6.1. A classificação de informações deve observar a publicidade como preceito geral e a atribuição do sigilo como exceção, conforme inciso I do artigo 3º da Lei 12.527/2011, de 18/11/2011 (Lei de Acesso à Informação), e o princípio da transparência, conforme consta no IN. OUVGER 01.008, de 26/08/2019;

8.6.2. As informações devem ser classificadas e tratadas segundo critérios e procedimentos estabelecidos em Instrumento Normativo que disponha sobre o assunto, atualmente o IN OUVGER 01.008/2022.

8.6.3. Os colaboradores devem observar as orientações do Instrumento Normativo supracitado para garantir o adequado tratamento às informações sigilosas, especialmente para evitar sua exposição indevida, o que começa com a adoção de cuidados básicos como, por exemplo, a guarda dos documentos em gavetas ou arquivos com tranca, a manutenção da mesa sem documentos ou informações sigilosas (mesa limpa) e a estação de trabalho bloqueada nos momentos de ausência de uso;

8.6.4. O tratamento de informação relacionado a pessoa natural identificada ou identificável, especialmente de dados pessoais sensíveis, deve observar as exigências e os princípios da Lei 13.709/2018, de 14/08/2018 (Lei Geral de Proteção de Dados), com destaque à necessidade de consentimento pelo titular e, para os princípios da finalidade, da adequação, da necessidade, da transparência, da segurança e da prevenção.

8.6.5. A disponibilidade e a proteção das informações devem ocorrer de acordo com a sua classificação e de forma a preservar a continuidade de negócios da Companhia;

8.6.6. Cláusulas de sigilo e confidencialidade devem constar nos contratos estabelecidos com profissionais terceirizados, prestadores de serviços e estagiários.

9. DA GESTÃO DE ACESSO

9.1. Toda concessão de acesso lógico e físico deve ser controlada por um método que envolva i**dentificação, autenticação e autorização**.

9.2. As atividades realizadas por meio de determinada credencial de acesso são de responsabilidade do seu respectivo usuário.

9.3. As instalações, equipamentos, redes e sistemas de tecnologia da informação, com exceção dos sistemas e portais destinados à divulgação pública de informações, devem estar equipados com mecanismos apropriados de controle de acesso físico e/ou lógico, permitindo a identificação das pessoas e/ou usuários que os utilizam.

9.4. Todos os recursos computacionais críticos da PortosRio devem ser mantidos em ambientes reservados, monitorados e com acesso físico controlado, sendo vedada a entrada de pessoas não autorizadas pela SUPTIN/GERSOL.

9.5. São considerados recursos computacionais críticos os servidores, *storages* e demais equipamentos e componentes acessórios utilizados para sustentar os serviços e sistemas de Tecnologia da Informação da PortosRio.

9.6. Os controles de acesso físico e lógico mencionados neste normativo aplicam-se exclusivamente às instalações e equipamentos de Tecnologia da Informação, não incluindo instalações portuárias ou administrativas da PortosRio.

9.7. Os detalhes relativos à gestão de acesso se encontram no **Anexo I - Gestão de Acesso (9520169).**

10. DA GESTÃO DO USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

10.1. Os recursos de tecnologia da informação disponibilizados pela PortosRio deverão ser utilizados em atividades relacionadas às funções institucionais, e abrangem os seguintes elementos:

10.1.1. Os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, os dispositivos móveis, as impressoras, copiadoras e equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios;

10.1.2. A rede corporativa, incluindo seus componentes físicos;

10.1.3. As contas de acesso dos usuários, assim como os certificados digitais;

10.1.4. Os sistemas e serviços tecnológicos desenvolvidos, adquiridos ou contratados, sob o regime de subscrição;

10.1.5. Os sistemas e serviços tecnológicos, na forma de software livre ou aberto, utilizados pela PortosRio; e

10.1.6. O acesso à internet.

10.2. A utilização dos recursos de tecnologia da informação será monitorada com a finalidade de detectar a ocorrência de eventos de segurança cibernética suspeitos e divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

10.3. Os detalhes relativos à gestão dos recursos de tecnologia da informação se encontram no **Anexo II - Gestão do uso dos recursos de TIC (9520183).**

11. GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

11.1. A Gestão de Incidentes em Segurança da Informação tem como objetivo garantir a identificação de fragilidades e incidentes, permitindo a adoção de medidas corretivas em tempo hábil.

11.2. Aos usuários dos recursos computacionais da PortosRio competem as seguintes responsabilidades:

11.2.1. Reportar prontamente à SUPTIN/GERSOL os incidentes em segurança da informação dos quais tenham conhecimento ou suspeita utilizando o e-mail etir@portosrio.gov.br; e

11.2.2. Colaborar, dentro de suas áreas de competência, na identificação e no tratamento de incidentes de segurança da informação.

11.3. As equipes da SUPTIN encarregadas do monitoramento dos ativos, serviços e sistemas devem notificar os incidentes identificados à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), para que sejam registrados e tratadas as devidas providências.

11.4. A PortosRio poderá receber notificações externas (CTIR.BR, CSIRT ou outras empresas) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, entre outros, os quais devem ser encaminhados à ETIR para o devido tratamento.

11.5. Os detalhes relativos à Gestão de Incidentes em Segurança da Informação se encontram no **Anexo III - Gestão e tratamento de Incidentes de SI (9520207)**

12. GESTÃO DE ATIVOS

12.1. São considerados ativos de Tecnologia da Informação:

12.1.1. **Ativos físicos:** Englobam os equipamentos e dispositivos que compõem a infraestrutura de Tecnologia da Informação e Comunicação. Isto inclui computadores, servidores, dispositivos de rede, unidades de armazenamento, periféricos e equipamentos de segurança, bem como suas respectivas instalações.

12.1.2. **Ativos de softwares:** Incluem todos os sistemas/programas, banco de dados e utilitários, utilizados para operar e gerenciar as operações de Tecnologia da Informação e Comunicação (TIC) de uma organização. Estes abrangem os softwares licenciados, personalizados ou desenvolvidos internamente para atender atividades administrativas e operacionais.

12.2. O planejamento da gestão de ativos de TIC deverá considerar os objetivos estratégicos, os requisitos legais e a estrutura física da PortosRio.

12.3. Todos os usuários devem adotar e estar cientes das boas práticas de segurança da informação para contribuir com a proteção e segurança dos ativos de TI utilizados pela PortosRio.

12.4. Os ativos de TI são destinados exclusivamente às atividades administrativas e operacionais da PortosRio, sendo vedada sua utilização para obtenção de benefícios pessoais, financeiros ou comerciais, assim como para prejudicar os serviços de TI institucionais.

12.5. Os detalhes relativos à Gestão de ativos de TIC se encontram **no Anexo IV - Gestão de Ativos de TIC (9520220).**

13. GESTÃO DE CONTINUIDADE

13.1. A gestão da continuidade dos serviços de TIC visa garantir que os serviços essenciais de TIC da PortosRio funcionem em níveis aceitáveis durante um incidente de segurança ou desastre, e que a recuperação total dos serviços seja realizada em um prazo minimamente aceitável.

13.2. O Processo de Gestão de Continuidade de TI encontra-se definido no Plano de Gestão de Continuidade de Serviços de TIC, disponibilizado no site institucional da PortosRio.

14. AUDITORIA E CONFORMIDADE

14.1. Para garantir o cumprimento das regras previstas nesta POSIC, bem como para fins de segurança e prevenção à fraude, a GERSOL reserva-se o direito de:

14.1.1. Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, internet, dispositivos móveis ou wireless, entre outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

14.1.2. Inspecionar qualquer arquivo que esteja em rede, no disco local da estação ou em qualquer outro ambiente para assegurar o rígido cumprimento desta POSIC;

14.1.3. Realizar, a qualquer tempo, a inspeção física nos computadores e demais ativos de TIC sob a responsabilidade da PortosRio;

14.1.4. Gerar e manter, de acordo com o tipo de sistema e com os recursos tecnológicos disponíveis, as trilhas de auditoria para rastreamento de possíveis falhas e fraudes;

14.1.5. Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;

14.1.6. Instalar câmeras de monitoramento nos locais destinados ao armazenamento e processamento de dados.

14.2. Os funcionários, prestadores de serviços, estagiários e demais colaboradores tomam ciência de que ambientes, recursos tecnológicos, sistemas, computadores, dispositivos móveis e redes da PortosRio estão sujeitos a monitoramento, atendendo à conformidade legal.

14.3. Os achados individuais resultantes de verificação de conformidade serão documentados e reportados ao Gestor da unidade verificada, para ciência e tomada das ações cabíveis.

14.4. Os resultados das auditorias devem ser documentados em relatórios detalhados e apresentados ao Comitê Gestor de Tecnologia da Informação e Comunicação – CGTIC para revisão e possíveis ações corretivas.

15. DAS RESPONSABILIDADES

15.1. **Compete ao CGTIC:**

15.1.1. Propor normas e procedimentos internos relativos à segurança da informação, em

conformidade com as legislações existentes sobre o tema.

15.1.2. Promover a cultura de segurança da informação na PortosRio através de campanhas de conscientização para os usuários internos e externos.

15.1.3. Garantir a publicação, atualização e aplicação das normas estabelecidas nesta POSIC.

15.2. **Compete à Superintendência de Tecnologia da Informação - SUPTIN:**

15.2.1. Indicar os membros que comporão a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da PortosRio.

15.2.2. Coordenar a instituição, implementação e manutenção da infraestrutura necessária à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da PortosRio.

15.2.3. Coordenar, junto as suas gerências subordinadas, a elaboração de instrumentos normativos sobre segurança da informação para os serviços e soluções de TIC da PortosRio

15.2.4. Assessorar na implementação das ações de Segurança da Informação e Comunicação.

15.2.5. Buscar apoio para prover os meios necessários à capacitação e ao aperfeiçoamento técnico dos membros da ETIR.

15.3. **Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR:**

15.3.1. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança da informação, divulgando práticas e recomendações;

15.3.2. Avaliar as condições de segurança da PortosRio por meio de verificações sistêmicas de conformidade e identificação de vulnerabilidades e artefatos maliciosos;

15.3.3. Pesquisar informações sobre novas ameaças a redes computacionais e soluções para mitigar os riscos e informar às áreas responsáveis; e

15.3.4. Comunicar incidentes de segurança aos órgãos competentes para fins estatísticos.

15.4. **Compete à Gerência de Operação de Soluções - GERSOL:**

15.4.1. Disciplinar os processos e responsabilidades a serem observados no gerenciamento de incidentes cibernéticos realizados pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da PortosRio.

15.4.2. Garantir a disponibilidade, confidencialidade, integridade, autenticidade, equidade e o privilégio mínimo das informações que tenham sido armazenadas por sistemas homologados pela GERCOS, seguindo esta POSIC.

15.4.3. Habilitar e manter o acesso à rede informatizada da PortosRio a todo usuário, considerando os níveis de acesso especificados pelas áreas.

15.4.4. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta POSIC.

15.4.5. Administrar, proteger e testar as cópias de segurança dos sistemas e informações relacionadas aos processos críticos e relevantes para a PortosRio.

15.4.6. Proteger continuamente todos os ativos de informação da empresa e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

15.4.7. Em caso de violação das políticas estabelecidas nesse documento, monitorar o acesso a recursos de TI, de forma que seja possível auditar e rastrear a identidade do usuário responsável.

15.4.8. Garantir, após o encaminhamento da GERARH, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida

restritiva para salvaguardar os ativos da empresa.

15.4.9. Elaborar, manter e publicar um Plano de Contingência de TI, com a finalidade de dirimir o impacto e os riscos de incidentes relacionados à segurança de TI.

15.4.10. Elaborar, manter e publicar um Plano de backup dos sistemas e informações relacionados aos processos críticos e relevantes para a PortosRio.

15.5. **Compete ao Gestor da unidade:**

15.5.1. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

15.5.2. Solicitar a alteração ou remoção dos níveis de acesso a sistemas e diretórios concedidos a empregado, estagiário ou jovem aprendiz, nos casos de transferência de setor ou sempre que necessária sua adequação às atividades desenvolvidas.

15.5.3. Prever em suas contratações que os dispositivos informatizados fornecidos e/ou utilizados pelo Contratado possuam os requisitos mínimos de segurança adotados pela PortosRio.

15.6. **Compete à Gerência de Administração de Recursos Humanos - GERARH:**

15.6.1. Informar à GERSOL e à GERCOS as ocorrências que justifiquem a ativação, bloqueio ou alteração no acesso de empregados à rede corporativa e sistemas informatizados da PortosRio, tais como:

a) Admissão.

b) Transferência de empregado.

c) Cessão de empregado.

d) Afastamento por licença não remunerada.

e) Afastamento por licença médica superior a 15 dias.

f) Férias.

g) Desligamento.

15.7. **Compete à Gerência de Gestão de Carreira - GERCAR**:

15.7.1. Informar à GERSOL e a GERCOS as ocorrências que justifiquem a ativação, bloqueio ou alteração no acesso de estagiários e jovens aprendizes à rede corporativa e sistemas informatizados da PortosRio, tais como:

a) Admissão.

b) Transferência de lotação.

c) Afastamento por licença médica superior a 15 dias.

d) Férias.

e) Desligamento.

15.8. **Compete aos Gestores e Fiscais de Contratos:**

15.8.1. Dar ciência do teor desta Política aos empregados terceirizados que estiverem atuando nos contratos sob sua responsabilidade.

15.8.2. Garantir que todos os empregados terceirizados sob sua fiscalização, cujas atividades envolvam acesso a informações sensíveis, confidenciais ou estratégicas, assinem o **Termo de Sigilo e Confidencialidade (9520237).**

15.8.3. As obrigações previstas neste item aplicam-se exclusivamente aos Gestores e Fiscais de Contratos responsáveis por serviços que demandem o acesso direto ou indireto a informações

classificadas como sensíveis, confidenciais ou estratégicas.

15.9. **Compete a todos os usuários de recursos informatizados da PortosRio:**

15.9.1. Zelar pela Segurança da Informação e Comunicação;

15.9.2. Acessar somente as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação desta política;

15.9.3. Manter inalterada a configuração dos equipamentos informatizados disponibilizados pela Companhia, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e Comunicação e pelas normas específicas da instituição. Qualquer alteração de configuração nos ativos de TI será considerada uma violação desta política;

15.9.4. Reportar imediatamente à ETIR (etir@portosrio.gov.br) quaisquer ocorrências ou suspeitas de incidentes de Segurança da Informação. Isso inclui vulnerabilidades, ameaças ou ações indevidas de que tenha conhecimento ou suspeita, relacionadas à segurança dos sistemas, serviços, informações ou qualquer recurso de TIC, mesmo que não estejam sob sua responsabilidade.

16. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

16.1. Caberá a ETIR, quando detectada uma violação, averiguar suas causas, consequências e circunstâncias nas quais ocorreu, verificando tanto se foi de um simples acidente, erro ou mesmo desconhecimento da política, como também se configurou um caso de negligência, ação deliberada ou fraudulenta. Essa averiguação possibilita o devido enquadramento de infração da conduta, assim como permite que as vulnerabilidades até então desconhecidas passem a ser consideradas, exigindo, se for o caso, alterações na política.

16.2. O descumprimento da POSIC poderá acarretar responsabilização, nos termos do IN ASSIND 01.012 e demais regulamentos da PortosRio e nos termos dos contratos ou convênios para estagiários, menores aprendizes, empresas prestadoras de serviço e seus empregados, sem prejuízo das responsabilidades civis e penais eventualmente cabíveis.

17. CONSIDERAÇÕES FINAIS

17.1. A POSIC deverá ser aprovada pela Diretoria Executiva e pelo Conselho de Administração.

17.2. A POSIC deverá ser formalmente publicada por Resolução e aplicada a todos os usuários de recursos informatizados da PortosRio.

17.3. Casos excepcionais ou não contemplados nesta POSIC deverão ser tratados individualmente, mediante orientação da SUPTIN.

17.4. A POSIC deve ser atualizada a cada dois anos, objetivando refletir os avanços tecnológicos e as alterações dos ambientes interno e externo.

18. ANEXOS

18.1. Anexo I - Gestão de Acesso (9520169).

18.2. Anexo II - Gestão do uso dos recursos de TIC (9520183).

18.3. Anexo III - Gestão e tratamento de Incidentes de SI (9520207).

18.4. Anexo IV - Gestão de Ativos de TIC (9520220).

18.5. Anexo V -Termo de Sigilo e Confidencialidade (9520237).

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br

PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

ANEXO I

Rio de Janeiro, 18 de março de 2025.

GESTÃO DE ACESSO

1. OBJETIVOS

1.1. O presente anexo complementa a Política de Segurança da Informação (POSIC) e define diretrizes para a gestão de identidade e controle de acesso, visando garantir níveis adequados de proteção aos ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) da PortosRio.

1.2. Esta norma está alinhada com os termos e diretrizes definidas na Política de Segurança da Informação (POSIC).

2. ABRANGÊNCIA

2.1. Esta Política se aplica a todas as informações em que a PortosRio seja o agente de tratamento, aos seus usuários, ao meio utilizado para este tratamento - seja digital ou físico - e às dependências físicas que abrigam os ativos críticos de informação. Especificamente, inclui:

2.1.1. Todos os funcionários, estagiários e jovens aprendizes contratados pela PortosRio;

2.1.2. Todos os contratados e terceiros que trabalham e acessam a rede e sistemas de informação da PortosRio;

2.1.3. Todos os servidores e agentes públicos de entidades fiscalizadoras que, em função de sua atividade, necessitam de acesso à rede e aos sistemas de informação da PortosRio;

2.1.4. Todos os ativos de hardware e software sob a responsabilidade da PortosRio; e

2.1.5. O datacenter e demais instalações destinadas à transmissão e ao processamento de dados sob a responsabilidade da SUPTIN.

2.2. Não fazem parte do escopo desta norma:

2.2.1. O controle e monitoramento do acesso físico à Sede da PortosRio, regulamentado pela IN GERSEG 15.011/2024

2.2.2. O controle e monitoramento do acesso físico ao edifício administrativo da PortosRio localizado na Av. Rodrigues Alves nº 20, regulamentado pela IN SUPGUA 13.007/2023

2.2.3. O controle e monitoramento do acesso físico aos Portos administrados pela PortosRio, regulamentado pela IN SUPGUA 13.001.01/2023

3. CONTROLE DE ACESSO LÓGICO

3.1. O controle de acesso lógico da PortosRio se baseia nos processos de **identificação**, **autenticação** e **autorização** para salvaguardar as informações da Instituição. Esses parâmetros são configurados durante a criação da conta do usuário

3.2. As contas dos usuários devem ser administradas através de aplicações de gerenciamento de diretórios corporativos, garantindo controle centralizado e seguro sobre acessos e permissões.

3.3. O acesso deve ser concedido e mantido pela GERSOL, baseado nas responsabilidades e

tarefas de cada usuário.

3.4. Identificação e Autenticação

3.4.1. A conta do usuário é constituída por suas credenciais de acesso (login e senha), informações relacionadas a sua respectiva lotação e perfil de acesso.

3.4.2. As credenciais de acesso abordadas nesta norma são pessoais e intransferíveis. Qualquer utilização ou tentativa de utilização não autorizada de credenciais de acesso poderá ser tratada como um incidente de segurança da informação.

3.4.3. Por padrão, a identificação do usuário será formada pelo <*primeiro_nome.ultimo_sobrenome*>, salvo na ocorrência de homônimos.

3.4.4. Nos casos em que o padrão adotado para identificação do usuário não seja possível, será utilizada outra combinação do nome completo do usuário. Não será admitida a utilização de apelidos como forma de identificação do usuário nos sistemas e serviços informatizados da PortosRio.

3.4.5. Por questões de segurança, será exigida a autenticação multifator para todas as credenciais de acesso aos recursos tecnológicos que dispuserem dessa tecnologia.

3.5. Perfis de acesso

3.5.1. Os perfis de acesso deverão ser definidos pela unidade requisitante à qual o usuário está vinculado, baseando-se no princípio do privilégio mínimo. Isso garante que os usuários acessem apenas o que é necessário para o desenvolvimento de suas atividades.

3.5.2. Caso seja necessário utilizar um perfil diferente do disponibilizado, a chefia imediata do usuário deverá encaminhar uma solicitação para a GERSOL, que analisará a requisição e poderá negá-la, motivadamente, se considerar desnecessária.

3.5.3. A GERSOL analisará eventuais solicitações de alteração de perfil e poderá negar a requisição, motivadamente, caso a considere desnecessária ou a mudança configurar um risco à segurança cibernética.

3.6. Criação de contas e concessão de acesso

3.6.1. A criação de uma nova conta de usuário e respectiva concessão de acesso deverá ser requerida através da abertura de chamado técnico e ocorrerá nos casos de:

I - Admissão de empregados, estagiários e jovens aprendizes;

II - Admissão de empregados terceirizados por empresa contratada, mediante solicitação e justificativa da fiscalização do contrato.

III - Cessão de empregados de outras instituições à PortosRio;

IV - Nomeação de membros do Conselho de Administração;

V - Nomeação de membros do Conselho Fiscal e do Comitê de Auditoria (COAUD);

VI - Designação de auditores de órgãos de controle para atuar na PortosRio; e

VII - Necessidade de criação de contas de serviço para a gestão de ativos físicos ou digitais.

3.6.2. As contas concedidas nos casos II e V do subitem anterior deverão possuir caráter temporário. O requisitante deve solicitar a revogação do acesso ao término do período de trabalho do usuário.

3.7. Diretrizes de acesso aos servidores corporativos

3.7.1. O acesso aos servidores corporativos deverá ser restrito aos usuários com privilégios administrativos, com a devida autorização concedida pela GERCOS e/ou GERSOL.

3.7.2. Sempre que possível, o controle de acesso aos servidores corporativos deve ser

implementado utilizando modelos baseados em funções (RBAC), onde as permissões são atribuídas a funções específicas em vez de a indivíduos, facilitando a gestão de acessos e a manutenção de segurança.

3.7.3. Todas as tentativas de acesso e operações críticas realizadas nos servidores corporativos devem ser monitoradas e registradas em logs de auditoria, permitindo a análise e identificação de atividades suspeitas ou não autorizadas.

3.7.4. Acessos e permissões dos usuários devem ser revisados periodicamente para assegurar que estão em conformidade com as responsabilidades atuais dos usuários e que acessos desnecessários ou não autorizados sejam revogados.

3.8. **Alteração e revogação de acesso**

3.8.1. A alteração e revogação de acesso à rede, serviços e aos sistemas computacionais disponibilizados pela PortosRio deverá ser requerida através da abertura de chamado técnico. O requisitante deverá informar o nome completo do usuário, a matrícula, o setor de lotação e os sistemas e serviços a serem habilitados ou desativados.

3.8.2. A alteração de uma conta de usuário ocorrerá nos casos de:

I - Transferência de lotação; e

II - Necessidade de adequação às atividades desenvolvidas.

3.8.3. A revogação de uma conta de usuário ocorrerá nos casos de:

I - Desligamento do empregado, estagiário ou jovem aprendiz;

II - Demissão do empregado terceirizado ou encerramento do contrato firmado com a PortosRio;

III - Licença sem vencimentos;

IV - Cessão para outro órgão ou entidade pública;

V - Licença médica por período superior a 15 dias; e

VI - Aposentadoria.

3.8.4. A solicitação de alteração e/ou revogação de conta é de responsabilidade da chefia imediata do usuário.

3.8.5. No caso previsto no subitem 4.7.3-II, caberá à Fiscalização do contrato solicitar a alteração e/ou revogação da conta do usuário.

3.8.6. A SUPTIN/GERSOL não se responsabilizará pelo acesso não autorizado nos casos em que não houver um registro formal de solicitação de revogação ou alteração.

3.8.7. Após o período de 180 dias, a conta revogada poderá ser permanentemente excluída do ambiente de dados da PortosRio, não sendo possível a sua reativação.

3.9. **Diretrizes de criação de senhas:**

3.9.1. A senha de acesso é o recurso inicial de autenticação do usuário na rede corporativa e demais sistemas e serviços informatizados. Ela é pessoal e intransferível, sendo proibida sua divulgação sob qualquer circunstância.

3.9.2. Toda a conta de usuário criada receberá uma senha temporária que possibilite o primeiro acesso. O usuário deverá realizar a troca imediata senha, atendendo aos seguintes requisitos mínimos:

I - Possuir 8 (oito) caracteres;

II - Possuir 1 (um) caractere maiúsculo (A-Z);

III - Possuir 1 (um) caractere minúsculo (a-z);

IV - Possuir 1 (um) número de 0 a 9;

V - Possuir 1 (um) caractere especial (@_&! $ # %=).

3.9.3. **Diretrizes de segurança das senhas:**

I - A senha não poderá ser igual às 5 (cinco) últimas senhas geradas pelo usuário.

II - Após cinco tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio será necessário que a chefia imediata do usuário abra um chamado técnico solicitando a sua reativação.

III - Os usuários podem alterar a própria senha e devem ser orientados a fazê-la, caso haja suspeita de uso indevido de suas credenciais.

IV - O usuário deve evitar a utilização de nomes, datas especiais e sequências óbvias de números e letras.

V - É obrigatório aos usuários, zelarem pela confidencialidade de sua senha de acesso, podendo ser responsabilizados pelas operações realizadas com a utilização de suas credenciais. Sob hipótese alguma as senhas devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);

VI - Todos os recursos tecnológicos adquiridos devem ter suas senhas iniciais alteradas imediatamente após a instalação.

VII - A periodicidade máxima para troca das senhas é 60 (sessenta) dias corridos.

4. CONTROLE DE ACESSO FÍSICO

4.1. Todas as instalações destinadas à transmissão e ao processamento de dados da PortosRio devem estar equipadas com mecanismos apropriados de controle de acesso físico e lógico, permitindo a identificação dos usuários. A entrada de pessoas não autorizadas pela SUPTIN/GERSOL é proibida.

4.2. Os usuários autorizados a acessar as instalações destinadas à transmissão e ao processamento de dados da PortosRio devem portar identificação visível e ter seu acesso registrado, incluindo data e hora de entrada e saída.

4.3. Devem ser implementados controles de monitoramento por imagem e autenticação utilizando, preferencialmente, reconhecimento facial e/ou biometria para validar todos os acessos.

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

4.5. As áreas restritas de TIC deverão permanecer livres de quaisquer equipamentos, materiais e/ou objetos que não sejam estritamente necessários à sua finalidade.

4.6. Não é permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio, ou outros equipamentos de gravação nas instalações destinadas à transmissão e ao processamento de dados da PortosRio, incluindo câmeras em dispositivos móveis, exceto se autorizado e registrado pela GERSOL.

4.7. **Da segurança ambiental do Data Center:**

4.7.1. A edificação do Data Center deve ser protegida contra descargas elétricas atmosféricas.

4.7.2. As portas das áreas de segurança do Data Center devem possuir mecanismos para fechamento automático.

4.7.3. Deve ser evitada a utilização de informações visuais que identifiquem as áreas de atividade de processamento e guarda das informações.

4.7.4. As portas e janelas do Data Center devem ser mantidas fechadas.

4.7.5. O Data Center deve dispor de sistema de fornecimento de energia elétrica redundante, incluindo nobreaks e geradores.

4.7.6. O ambiente deve possuir sistema de refrigeração com controle de temperatura e umidade, compatível com a necessidade dos equipamentos instalados.

4.7.7. Deve ser previsto sistema de combate a incêndio compatível com a área e os equipamentos do Data Center, incluindo detectores de fumaça e extintores adequados.

5. DOCUMENTOS RELACIONADOS

5.1. Política de Segurança da Informação (9520132).

Documento assinado eletronicamente por **Juliana De Araujo De Toledo**, **Especialista Portuário**, em 18/03/2025, às 13:43, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.transportes.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **9520169** e o código CRC **B12F450B**.

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br

PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

ANEXO II

Rio de Janeiro, 18 de março de 2025.

GESTÃO DO USO DOS RECURSOS DE TIC

1. OBJETIVOS

1.1. O presente anexo complementa a Política de Segurança da Informação (POSIC) da PortosRio, estabelecendo diretrizes específicas para a gestão do uso dos recursos de Tecnologia da Informação e Comunicação (TIC) para assegurar que todos os usuários utilizem os recursos de TIC de forma responsável, conforme as melhores práticas de segurança e conformidade regulatória.

1.2. São objetivos da Gestão do uso de Recursos de TIC:

1.2.1. Promover o uso responsável e eficiente dos recursos tecnológicos, assegurando que sejam utilizados exclusivamente para finalidades relacionadas às atividades da PortosRio.

1.2.2. Implementar práticas de segurança da informação que garantam a confidencialidade, integridade e disponibilidade dos dados e sistemas da PortosRio.

1.2.3. Estabelecer controles e procedimentos para proteger os ativos de TIC contra acessos não autorizados, danos acidentais ou maliciosos, e outros riscos de segurança.

1.2.4. Garantir que o uso dos recursos de TIC esteja em conformidade com as políticas internas, regulamentos externos e melhores práticas de segurança da informação.

1.2.5. Facilitar a auditoria e monitoramento do uso dos recursos de TIC para assegurar a conformidade contínua e detectar eventuais desvios.

1.2.6. Informar e educar os usuários sobre as diretrizes e melhores práticas para o uso seguro e eficiente dos recursos de TIC.

1.2.7. Fomentar uma cultura organizacional de segurança da informação, onde todos os usuários compreendem e respeitam as políticas e procedimentos estabelecidos.

2. ABRANGÊNCIA

2.1. Esta norma se aplica a todos os usuários dos recursos computacionais da PortosRio e inclui a rede local, dispositivos de hardware, software, serviços de comunicação e demais ativos tecnológicos da Companhia.

3. RECURSOS DE HARDWARE

3.1. **Estações de Trabalho:**

3.1.1. As estações de trabalho fornecidas pela PortosRio devem ser utilizadas nas atividades profissionais do usuário, sendo permitido o uso pessoal desde que em conformidade com critérios de razoabilidade e responsabilidade. No entanto, a GERSOL não é responsável pela salvaguarda de dados pessoais eventualmente armazenados nesses dispositivos.

3.1.2. Toda estação de trabalho fornecida pela PortosRio deverá:

a) Possuir uma suíte de proteção (antivírus) instalada e atualizada;

b) Estar configurado no domínio *portosrio.gov.br*;

c) Exigir credenciais de acesso na inicialização do sistema operacional;

d) Ter suas portas USB desabilitadas.

3.1.3. Todo e qualquer processo de manutenção, instalação, configuração, desinstalação, substituição ou remanejamento de qualquer estação de trabalho, ainda que parcial, deve ser realizado pela GERSOL ou sob sua supervisão.

3.1.4. Não será realizado procedimento de backup das estações de trabalho.

3.1.5. É vedado aos usuários:

a) Proceder à abertura ou manuseio de qualquer ativo pertencente à PortosRio, com a finalidade de realização de qualquer tipo de reparo;

b) Conectar dispositivos de comunicação (modens celulares e similares) de origem externa nos ativos da PortosRio, exceto nos casos autorizados;

c) Desinstalar programas, aplicativos, recursos, ferramentas ou *plugins* da PortosRio, seja por qualquer motivo, sem a devida autorização e acompanhamento da GERCOS ou GERSOL.

3.1.6. Todo arquivo gerado em função do trabalho na PortosRio deve ser armazenado em diretório de rede, sendo vedada sua manutenção em disco local na estação de trabalho. Em caso de descumprimento dessa exigência, a GERSOL não se responsabilizará pela perda de dados armazenados localmente.

3.1.7. Ao final do expediente, o usuário deverá desligar o computador corretamente, utilizando a função de desligamento do sistema operacional.

3.2. **Computadores portáteis (notebooks):**

3.2.1. Os computadores portáteis deverão ser configurados com os mesmos requisitos de segurança estabelecidos para as estações de trabalho.

3.2.2. O fornecimento de computadores portáteis está condicionado à disponibilidade do recurso e à necessidade de trabalho do usuário fora das dependências da PortosRio, mediante solicitação do titular da unidade e assinatura do Termo de Responsabilidade (Anexo II-A).

3.2.3. O usuário responsável pelo notebook deve mantê-lo em local seguro quando não estiver em uso, garantindo que não seja acessado indevidamente por terceiros.

3.2.4. Em caso de desligamento ou término das atividades que motivaram o fornecimento do equipamento, o mesmo deve ser devolvido à GERSOL, com todos os acessórios que o acompanharam, no prazo de 5 (cinco) dias corridos.

3.2.5. Nos casos de devolução, a GERSOL realizará uma vistoria técnica para avaliar as condições físicas do equipamento entregue e emitirá o Termo de Devolução de Equipamento (Anexo II-B).

3.2.6. É vedada a transferência direta do equipamento fornecido para outro usuário sem a realização de uma vistoria prévia da GERSOL.

3.2.7. A GERSOL poderá realizar, a qualquer tempo, inspeção para verificar os aspectos relativos à configuração e à segurança dos computadores portáteis.

3.3. **Impressoras e Multifuncionais:**

3.3.1. As impressoras e equipamentos multifuncionais disponibilizados pela PortosRio são de uso coletivo e devem ser instalados em áreas de acesso compartilhado, visando promover o uso sustentável por todos os colaboradores.

3.3.2. Todos os equipamentos devem ser configurados, por padrão, para executar o recurso de impressão segura, garantindo assim a proteção contra o acesso indevido aos documentos impressos.

3.3.3. Todo usuário é responsável por garantir a segurança dos documentos impressos, copiados ou digitalizados sob sua responsabilidade. Para garantir o sigilo e a confidencialidade no uso dos equipamentos de impressão, o usuário deverá:

a) Utilizar a função "impressão segura" ou outra semelhante, para a liberação de impressões;

b) Descartar adequadamente os documentos pessoais ou sigilosos após o uso, empregando métodos seguros de destruição, como trituradores de papel, para prevenir o acesso não autorizado às informações; e

c) Recolher os documentos imediatamente após sua impressão ou digitalização, evitando que informações sensíveis fiquem expostas.

3.3.4. É estritamente proibido o uso das impressoras e multifuncionais para a reprodução de materiais protegidos por direitos autorais, ilegais, difamatórios, obscenos ou que violem quaisquer leis ou políticas internas da PortosRio.

3.4. **Equipamentos de rede e servidores:**

3.4.1. O acesso e manuseio dos equipamentos de rede e servidores é restrito aos empregados da GERSOL com perfil de administrador ou a prestadores de serviços, sob a sua supervisão.

3.4.2. Os equipamentos de rede e servidores devem ser monitorados continuamente, de modo a se obter um acompanhamento permanente dos acessos, das atividades administrativas e das condições de integridade e performance dos equipamentos.

3.4.3. Todas as configurações padrão de fábrica devem ser alteradas, incluindo senhas, nomes de usuário e configurações de rede.

3.4.4. Todos os equipamentos devem ter as configurações de segurança recomendadas implementadas, o que inclui a desativação de serviços desnecessários, a utilização de protocolos seguros e a segmentação da rede.

3.4.5. Recomenda-se a aplicação regular de patches e atualizações de firmware e software para corrigir vulnerabilidades conhecidas.

4. RECURSOS DE SOFTWARE

4.1. **Propriedade e uso de software:**

4.1.1. Todos os sistemas aplicativos, desenvolvidos ou adquiridos pela PortosRio, são de sua exclusiva propriedade e sua utilização é restrita ao apoio das atividades da Instituição.

4.2. **Instalação de software:**

4.2.1. Apenas softwares aprovados e licenciados pela SUPTIN e suas gerências subordinadas podem ser instalados nos dispositivos corporativos.

4.2.2. O uso de software para fins pessoais nos dispositivos corporativos é estritamente proibido. Somente ferramentas e softwares necessários para a realização das tarefas profissionais devem ser utilizados.

4.3. **Manutenção e atualização de software:**

4.3.1. Todos os softwares instalados devem ser mantidos atualizados com os patches e atualizações de segurança mais recentes, exceto quando a atualização inviabilizar ou prejudicar o uso de outros sistemas.

4.3.2. Para softwares críticos, a aplicação de patches deve ser testada em um ambiente controlado antes da implementação em produção para garantir que o procedimento não cause interrupções ou problemas de compatibilidade.

4.4. **Uso ilegal e distribuição não autorizada:**

4.4.1. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela GERSOL.

4.5. **Contratação e desenvolvimento de novos sistemas:**

4.5.1. Na contratação ou no desenvolvimento de novos sistemas para o uso da PortosRio, recomenda-se incluir os seguintes requisitos:

a) Autenticação baseada na integração com o Active Directory da PortosRio, para usuários internos do sistema.

b) Suporte à autenticação multifator (MFA) para todos os usuários.

c) Utilização do protocolo HTTPS na comunicação entre o usuário e o servidor para proteger os dados em trânsito.

d) Utilização de criptografia forte (por exemplo, TLS) para proteger dados em trânsito e em repouso.

5. SERVIÇOS DE TIC

5.1. **Rede Corporativa:**

5.1.1. O acesso à rede corporativa é concedido exclusivamente aos usuários de recursos computacionais que, em função de suas atividades, necessitem acessar a rede e os sistemas de informação da PortosRio, mediante a utilização de suas respectivas credenciais.

5.1.2. A credencial de acesso do usuário é pessoal e intransferível, sendo proibida a utilização da conta de terceiros para acessar a rede da PortosRio.

5.1.3. Antes de se ausentar do seu local de trabalho, o usuário deve realizar *logoff* em todos os sistemas em uso e bloquear sua área de trabalho, a fim de evitar o acesso por pessoas não autorizadas.

5.1.4. As estações de trabalho devem ser configuradas para bloquear automaticamente após 5 minutos de ociosidade.

5.1.5. Não são permitidas alterações das configurações de rede e na inicialização dos equipamentos.

5.1.6. É vedado o acesso à rede corporativa por meio de computadores não fornecidos pela PortosRio.

5.2. **Internet :**

5.2.1. A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, de modo a contribuir para o desenvolvimento de atividades relacionadas à PortosRio.

5.2.2. Toda estação de trabalho inspecionada e homologada pela GERSOL terá acesso controlado à Internet.

5.2.3. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a PortosRio, em conformidade com a legislação vigente, reserva-se o direito de monitorar e registrar todos os acessos.

5.2.4. É vedado aos usuários, no uso do serviço de internet:

a) Utilizar programas ou *plugins* de camuflagem de navegação, deleção de histórico de navegação, de desvio de proxy e/ou tunelamento de navegação;

b) Abrir arquivos executáveis, com a extensão *.exe*, ou equivalentes, não autorizados pela PortosRio;

c) Efetuar o upload indevido de qualquer conteúdo de propriedade da PortosRio;

d) Acessar sites ou programas de compartilhamento de arquivos do tipo P2P, tais como, Skype, BitTorrent e o Emule, por exemplo;

e) Acessar sites de jogos on-line ou stand-alone (sem conexão de Internet);

f) Acessar sites que menosprezem, depreciem ou incitem o preconceito a determinadas

classes;

g) Acessar sites que possibilitem a distribuição de informações de nível restrito ou sigiloso;

h) Acessar sites que permitam a transferência (downloads) de arquivos e/ou programas ilegais e;

i) Acessar sites de pornografia, pedofilia e incitação ao terrorismo.

5.2.5. O acesso e uso de mídias sociais a partir da rede corporativa da PortosRio é permitido somente aos usuários lotados na ASSCOM, no estrito exercício de suas atividades.

5.2.6. O acesso e uso de sites da categoria "áudio/vídeo" será concedido temporariamente e apenas para atividades relacionadas ao treinamento de empregados e palestras de interesse da PortosRio, mediante abertura de chamado técnico.

5.2.7. No caso de um site bloqueado, cujo conteúdo esteja em conformidade com as regras e diretrizes do presente documento, o usuário pode solicitar a liberação de acesso junto a GERSOL, mediante abertura de chamado técnico.

5.3. **Internet sem fio (Wi-Fi):**

5.3.1. A PortosRio disponibilizará o acesso à rede de internet sem fio aos seus usuários e visitantes em áreas de uso comum, salvo nos casos de inviabilidade tecnológica.

5.3.2. A rede de internet sem fio deverá ser segregada, garantido, assim, o isolamento da rede interna da PortosRio.

5.3.3. As redes sem fio devem ser configuradas utilizando criptografia WPA3, sempre que possível, para garantir a segurança das comunicações.

5.3.4. O acesso à Internet por meio das redes sem fio observará as regras dispostas no item 6.2 desta norma, contudo, por questões de segurança tecnológica, regras específicas poderão ser implementadas.

5.3.5. Os acessos à rede sem fio poderão ser bloqueados, temporariamente ou por tempo indeterminado, nos casos em que for identificado um eventual risco à segurança tecnológica.

5.4. **Site institucional, intranet e sistemas web:**

5.4.1. O site institucional e a intranet corporativa deverão ser protegidos por criptografia TLS/SSL para evitar interceptação e acesso não autorizado.

5.4.2. Toda estação de trabalho inspecionada e homologada pela GERSOL terá acesso irrestrito à intranet corporativa e ao site institucional da PortosRio.

5.4.3. A Intranet da PortosRio possui recursos de Gerenciamento de Conteúdo. Para maiores detalhes sobre como publicar informações, deve-se utilizar o IN.OUVGER.01.008 e o IN.OUVGER.01.009 como referência.

5.4.4. O Gerenciador de Conteúdo deverá manter os dados de cada publicação criada, com a finalidade de identificar o autor e a data da publicação. É proibida a publicação de conteúdo diferente do especificado para cada área, conforme o exposto no IN.OUVGER.01.009.

5.5. **E-mail Corporativo:**

5.5.1. É conferido a todo empregado da PortosRio em exercício, uma conta de e-mail institucional, sob o domínio oficial da PortosRio (portosrio.gov.br), destinada a finalidades profissionais.

5.5.2. As contas de e-mail institucional poderão ser do tipo:

a) Individual, pertencente ao usuário da PortosRio;

b) Setorial, para envio de comunicações em nome da Unidade; e

c) Temporária, para o uso em campanhas e comissões de caráter temporário.

5.5.3. As contas de e-mail setoriais e temporárias deverão ser criadas, preferencialmente, a partir do recurso de caixa compartilhada, quando houver disponibilidade tecnológica para essa finalidade.

5.5.4. A conta de e-mail institucional será vinculada à conta corporativa do usuário, utilizando as mesmas credenciais (nome de usuário e senha) já cadastradas e, no mínimo, um segundo fator de autenticação. Ela é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências.

5.5.5. É proibido o uso de provedores de e-mail externos para encaminhamento de mensagens de correio eletrônico da PortosRio.

5.5.6. É de responsabilidade do usuário efetuar periodicamente a manutenção de sua caixa postal.

5.5.7. É vedada a utilização do e-mail institucional para:

a) Enviar mensagem cujo conteúdo possa gerar, de forma direta ou indireta, riscos à imagem institucional da PortosRio;

b) Realizar cadastros para fins pessoais (comércio, acessos a sites, etc.);

c) Reenviar ou propagar mensagens em cadeia (correntes), independentemente da vontade do destinatário de receber tais mensagens;

d) Utilizá-lo com objetivos político-partidários, religiosos, entre outros;

e) Abrir mensagens consideradas suspeitas ou caracterizadas como spam e *phishing scam;*

f) Abrir e-mail que contenham arquivos anexos com as extensões .bat, .exe, .src, .lnk.

g) Produzir, armazenar, transmitir ou divulgar mensagem que:

I - Que não sejam compatíveis com a missão, visão e valores da PortosRio;

II - Represente uma quebra da confidencialidade de informações relacionadas à PortosRio ou aos terceiros com as quais mantenham relação;

III - Caracterize invasão da privacidade e/ou intimidade de terceiros.

5.5.8. O bloqueio da conta de e-mail institucional do usuário ocorrerá nos seguintes casos:

a) Desligamento do empregado;

b) Afastamento do empregado motivado pela concessão de licença não remunerada; e

c) Cessão do empregado a outro órgão ou entidade governamental.

5.5.9. O bloqueio é realizado pela GERSOL, na comunicação do desligamento do usuário, efetuada pela GERARH.

5.5.10. Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar 30MB.

5.5.11. A caixa de e-mail do usuário será mantida, após a desativação, pelo período de 30 dias, não sendo possível a sua recuperação após desse prazo.

5.5.12. A GERSOL poderá, a qualquer tempo, rastrear ou varrer o conteúdo das mensagens, de forma automática, por softwares especiais, a fim de verificar se os conteúdos das mesmas estão de acordo com o disposto nesta norma.

5.6. **Armazenamento e compartilhamento de arquivos:**

5.6.1. Todos os arquivos, produzidos ou armazenados, relacionados ao trabalho na PortosRio, devem ser mantidos em plataforma centralizada destinada a essa finalidade, sendo vedada a manutenção de documentos corporativos em estações de trabalho.

5.6.2. Cada setor terá uma pasta exclusiva e restrita aos usuários da unidade para a gestão dos

seus respectivos documentos. Os usuários poderão visualizar, armazenar e excluir arquivos e subpastas criados na pasta do setor.

5.6.3. Nos casos de necessidade de armazenamento de informações restritas e sigilosas, o usuário deverá solicitar a criação de uma pasta sigilosa, informando o motivo e os usuários que poderão acessá-la. A solicitação deverá ser feita por meio de abertura de chamado técnico.

5.7. **Acesso remoto:**

5.7.1. O acesso remoto será concedido mediante autorização da chefia imediata do usuário e após avaliada a sua real necessidade pela GERSOL.

5.7.2. A concessão de uso de acesso remoto será limitada às necessidades do usuário, com o intuito de atender aos objetivos de negócio da PortosRio, sendo vedado o acesso para outras finalidades e em horário diverso ao período regular de trabalho.

5.7.3. A autorização para a concessão do acesso remoto concedido deverá levar em consideração critérios objetivos e criteriosos, de forma a garantir que somente o mínimo necessário para a boa execução das atividades seja autorizado.

5.7.4. Todo acesso à rede corporativa da PortosRio realizado fora de suas dependências (acesso remoto) deverá ser rigorosamente controlado, utilizando criptografia por uma VPN e duplo fator de autenticação.

5.7.5. O usuário que utiliza os recursos de acesso remoto ao ambiente corporativo da PortosRiodeve proteger suas credenciais de acessos e realizar o encerramento da sessão ao término de suas atividades.

5.7.6. A GERSOL pode desabilitar ou restringir as condições de acesso remoto de qualquer usuário que descumprir com as disposições do presente documento, demonstrar incapacidade ou negligência no uso desta facilidade tecnológica.

6. DOCUMENTOS RELACIONADOS

6.1. Política de Segurança da Informação (9520132).

7. ANEXO II - A: MODELO DE TERMO DE RESPONSABILIDADE

TERMO DE RESPONSABILIDADE

DADOS DO EMPREGADO		
EMPREGADO:	**REGISTRO**	**LOTAÇÃO**
FUNÇÃO:	**ÁREA**	**TELEFONE:**

DADOS DO EQUIPAMENTO			
FABRICANTE:	**MODELO:**	**PATRIMÔNIO/Nº DE SÉRIE:**	**ESTADO:** ( )NOVO ( ) USADO

ITENS INCLUSOS: ( ) CARREGADOR ( ) BATERIA (INTERNA) ( ) MOUSE ( ) OUTROS: < Descrever quais acessórios adicionais foram entregues>

REGRAS DE UTILIZAÇÃO
1. O equipamento deverá ser utilizado ÚNICA e EXCLUSIVAMENTE a serviço da empresa tendo em vista a atividade a ser exercida pelo EMPREGADO; 2. Ficará o EMPREGADO obrigado a dedicar os cuidados necessários pelo uso e conservação do equipamento, bem como ligar, operar e desligar conforme as recomendações e especificações de seu fabricante; 3. O EMPREGADO tem somente a DETENÇÃO, tendo em vista o uso exclusivo para prestação de serviços profissionais e NÃO a PROPRIEDADE do equipamento, sendo terminantemente proibido o empréstimo, aluguel ou cessão deste a terceiros; 4. Ao término do contrato individual de trabalho ou da atividade que justificou o fornecimento do bem, o empregado se compromete a devolver, à Gerência de Operação de Soluções – GERSOL, o equipamento e seus acessórios livres de bloqueios/codificações e em perfeito estado de conservação, considerando-se o desgaste natural pelo seu uso normal, em um prazo máximo de 5 (cinco) dias corridos; 5. Se o equipamento e/ou acessórios for danificado ou extraviado por descuido do EMPREGADO, este deverá comunicar imediatamente à GERSOL para providências quanto à reposição junto à CONTRATADA e estará sujeito a processo de apuração de responsabilidade; 6. Se o equipamento e/ou acessórios for roubado ou furtado, o EMPREGADO deverá registrar boletim de ocorrência na Polícia Civil e comunicar imediatamente à GERSOL para providências quanto à reposição junto à CONTRATADA.

Declaro estar ciente de que a não observância das regras de utilização, perda ou extravio do aparelho e seus acessórios por culpa exclusiva do empregado, será objeto de apuração e eventual aplicação das penalidades cabíveis, bem como indenização do valor do bem, nos termos do IN ASSIND 01.012.

<NOME DO USUÁRIO DETENTOR DO EQUIPAMENTO>
<REGISTRO>

8. ANEXO II - B: MODELO DE TERMO DE DEVOLUÇÃO

TERMO DE DEVOLUÇÃO DE EQUIPAMENTO

DADOS DO EMPREGADO		
EMPREGADO:	**REGISTRO**	**LOTAÇÃO**
FUNÇÃO:	**ÁREA**	**TELEFONE:**

DADOS DO EQUIPAMENTO

DADOS DO EQUIPAMENTO		
FABRICANTE:	**MODELO:**	**PATRIMÔNIO/Nº DE SÉRIE:**
ITEM	**ESTADO**	**OBSERVAÇÃO**
( ) NOTEBOOK	( ) BOM ( ) REGULAR ( ) DEFICIENTE ( ) CRÍTICO	
( ) CARREGADOR	( ) BOM ( ) REGULAR ( ) DEFICIENTE ( ) CRÍTICO	
( ) BATERIA (INTERNA)	( ) BOM ( ) REGULAR ( ) DEFICIENTE ( ) CRÍTICO	
( ) MOUSE	( ) BOM ( ) REGULAR ( ) DEFICIENTE ( ) CRÍTICO	
( ) OUTROS*	( ) BOM ( ) REGULAR ( ) DEFICIENTE ( ) CRÍTICO	
Legenda: **Bom:** O equipamento está em boa condição. **Regular**: O equipamento está em condição aceitável, com alguns defeitos ou desgastes, mas ainda operável. **Deficiente**: O equipamento está em condição insatisfatória, com vários defeitos ou desgastes que afetam seu funcionamento. **Crítico**: O equipamento está em condição muito ruim, com defeitos ou desgastes graves que comprometem seu uso.		

*Inclua novas linhas à tabela, caso haja outros itens a serem descritos

Declaro que o equipamento supracitado e demais componentes foram devolvidos nas condições acima avaliadas, estando o empregado detentor de sua posse sujeito às penalidades previstas no IN ASSIND 01.012., em caso de extravio ou avaria por descuido ou mau uso.

<NOME DO AVALIADOR>
<REGISTRO>

<NOME DO USUÁRIO DETENTOR DO EQUIPAMENTO>
<REGISTRO>

Documento assinado eletronicamente por **Juliana De Araujo De Toledo**, **Especialista Portuário**, em 18/03/2025, às 13:43, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.transportes.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **9520183** e o código CRC **DB5565FE**.

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br

PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

ANEXO III

Rio de Janeiro, 18 de março de 2025.

GESTÃO E TRATAMENTO DE INCIDENTES DE SI

1. OBJETIVOS

1.1. O presente anexo complementa a Política de Segurança da Informação (POSIC) da PortosRio com o intuito de estabelecer princípios, conceitos e diretrizes para a administração de eventos ou incidentes de segurança. Ela orienta o processo de gestão de incidentes de segurança cibernética , garantindo que sejam tratados adequadamente, com o objetivo de minimizar os impactos para o negócio.

1.2. Esta norma está alinhada com os termos e diretrizes definidas na Política de Segurança da Informação (POSIC).

2. ABRANGÊNCIA

2.1. Esta norma abrange os serviços referentes ao tratamento de incidentes da segurança da informação no intuito de atender as necessidades de segurança da informação

3. DIRETRIZES GERAIS:

3.1. São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio da PortosRio e seus objetivos em risco.

3.2. Todos os usuários devem ser capazes de identificar incidentes de segurança da informação quando os presenciarem.

3.3. São considerados eventos ou fragilidades de segurança cibernética:

3.3.1. Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, integridade ou disponibilidade do ambiente da organização;

3.3.2. Indisponibilidade do ambiente tecnológico em virtude de ataques maliciosos internos ou externos;

3.3.3. Vazamento de informações confidenciais, como dados de clientes ou informações estratégicas;

3.3.4. Tentativas internas ou externas de obter acesso não autorizado a sistemas ou dados, ou de comprometer o ambiente de TI;

3.3.5. Atos que violem explicitamente ou implicitamente uma política de segurança;

3.3.6. Uso ou acesso não autorizado a um sistema;

3.3.7. Modificações em um sistema sem o conhecimento, instruções ou consentimento prévio do proprietário do sistema; e

3.3.8. Compartilhamento de senhas.

3.4. Suspeitas de vulnerabilidades ou fragilidades não devem ser testadas ou provadas pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

3.5. Todos os incidentes de segurança devem ser registrados, classificados e tratados.

3.6. Todos os incidentes e ações tomadas devem ser documentados de forma detalhada e precisa

3.7. As lições aprendidas devem ser utilizadas para melhorar os procedimentos e fortalecer a postura de segurança da PortosRio.

4. PROCESSO DE GESTÃO DE INCIDENTES

4.1. O Processo de Gestão de Incidentes deverá ser elaborado pela SUPTIN, contemplando as seguintes etapas:

4.1.1. **Identificação e Registro:** Envolve a detecção ou recebimento de notificação de incidente de segurança em redes computacionais, seu registro, e obtenção das autorizações necessárias para iniciar a investigação.

4.1.2. **Investigação e Contenção**: Abrange a investigação e tratamento do incidente, coleta e preservação de evidências, comunicação às áreas afetadas, e proposição e aplicação de ações de contenção, quando necessárias.

4.1.3. **Encerramento:** Inclui a análise do incidente, verificação da necessidade de ações adicionais, providências ou comunicações, e, após o cumprimento dessas etapas, o encerramento do incidente.

4.1.4. **Avaliação de incidentes:** Consiste na análise do histórico de incidentes, consolidação das informações e indicadores, e na identificação de oportunidades de melhoria e lições aprendidas.

4.2. A comunicação sobre o incidente e o processo de tratamento às partes interessadas dependerá da sua classificação, nível de criticidade e informações envolvidas, podendo incluir autoridades agentes internos e externos da PortosRio.

4.3. O tratamento da informação deve ser conduzido de modo a garantir a disponibilidade, integridade, confidencialidade e autenticidade dos dados, assegurando o retorno das operações à normalidade no menor prazo possível. Além disso, deve-se evitar futuras ocorrências por meio da proposição de ações corretivas, quando necessárias.

4.4. Os incidentes, notificados ou detectados, deverão ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

4.5. O acesso às evidências e relatório de incidentes de segurança da informação é permitido apenas à área de Gestão de TI, DPO e aos Gestores diretamente envolvidos nos incidentes.

4.6. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o GCTIC deverá ser comunicado para avaliação das providências cabíveis.

5. DOCUMENTOS RELACIONADOS

5.1. Política de Segurança da Informação (9520132)

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br

PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

ANEXO IV

Rio de Janeiro, 18 de março de 2025.

PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

ANEXO IV

GESTÃO DE ATIVOS DE TIC

1. OBJETIVOS

1.1. O presente anexo complementa a Política de Segurança da Informação (POSIC) e define diretrizes e procedimentos para a gestão eficiente dos ativos de Tecnologia da Informação e Comunicação (TIC) da PortosRio, garantindo sua utilização adequada, manutenção, segurança e descarte.

1.2. Esta norma está alinhada com os termos e diretrizes definidas na Política de Segurança da Informação (POSIC).

2. ABRANGÊNCIA

2.1. Esta Política se aplica a todos os ativos de tecnologia da informação da PortosRio, incluindo hardware, software, dados e qualquer outro recurso de TI utilizado pelos empregados e demais colaboradores.

3. DIRETRIZES GERAIS

3.1. São considerados ativos de Tecnologia da Informação da PortosRio:

3.1.1. **Ativos físicos**

I - Computadores de mesa (desktops);

II - Notebooks e laptops;

III - Servidores;

IV - Dispositivos móveis (smartphones, tablets);

V - Impressoras e scanners;

VI - Equipamentos de rede (firewalls, roteadores, switches);

VII - Equipamentos de comunicação (modems, antenas, hubs)

VIII - Equipamentos de armazenamento (discos rígidos, SSDs, NAS);

IX - Monitores e periféricos (teclados, mouses, câmeras);

X - Equipamentos de backup (fitas de backup, dispositivos de backup em nuvem); e

XI - Equipamentos de segurança (firewalls, dispositivos de autenticação).

3.1.2. **Ativos digitais:**

I - Sistemas operacionais (Windows, Linux, macOS)

II - Software de produtividade (Microsoft Office, Google Workspace)

III - Aplicações empresariais (ERP, CRM)

IV - Ferramentas de desenvolvimento (IDEs, bibliotecas de software)

V - Sistemas relacionados a infraestrutura de TI (softwares de virtualização, monitoramento, gerenciamento de rede, backup e segurança);

VI - Sistemas de gestão de banco de dados; e

VII - Serviços em nuvem (IaaS, PaaS, SaaS).

3.2. A contratação ou aquisição de ativos de TI deverá seguir as diretrizes estabelecidas no IN GERCOS 10.003/2023.

3.3. A aquisição e o descarte de ativos físicos devem ser realizados considerando o ciclo de vida útil do material, em conformidade com a Portaria SGD/MGI nº 2.715, de 21 de junho de 2023, e o documento de Boas Práticas, Orientações e Vedações, vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, ambos com força normativa legal.

3.4. O ambiente físico dos ativos de TI deve ser adequado aos requisitos técnicos do ativo e ter a segurança física adequada ao valor do respectivo ativo de informação e aos riscos identificados.

3.5. O orçamento da SUPTIN deve considerar a necessidade de taxa de renovação de ativos de 20% ao ano.

3.6. O planejamento da aquisição e gestão dos ativos de TI deve estar alinhado com o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC vigente.

3.7. Todos os ativos de TI com armazenamento de dados deverão ser analisados criticamente antes de serem enviados para manutenção, serem descartados, doados, remanejados ou reutilizados, com a finalidade de assegurar a proteção e confidencialidade das informações existentes

3.8. O processo de inventário dos ativos de TI da PortosRio deve seguir os mesmos procedimentos aplicáveis aos demais bens móveis, regulamentados pelo Instrumento Normativo GERAIP 17.001 - Gerir Patrimônio.

4. MAPEAMENTO DE ATIVOS:

4.1. O processo de mapeamento de ativos de informação objetiva estruturar e manter registros de ativos de informação para subsidiar os processos de gestão de riscos, gestão de continuidade e gestão de mudanças nos aspectos relativos à segurança da informação.

4.2. Sempre que possível, os ativos de TI devem ser identificados de modo a permitir seu mapeamento via software, para monitoramento e controle de inventário.

4.3. Os ativos de TI devem ser monitorados para garantir seu funcionamento adequado e fornecer informações para o gerenciamento de capacidade e demanda, para remanejamento e descarte.

5. UTILIZAÇÃO DOS ATIVOS

5.1. Os ativos de TIC devem ser utilizados exclusivamente para fins profissionais, conforme as políticas e diretrizes da PortosRio.

5.2. O uso inadequado, abusivo ou não autorizado de ativos de TIC é estritamente proibido e

sujeito a medidas disciplinares.

6. MANUTENÇÃO E SUPORTE

6.1. A manutenção preventiva e corretiva dos ativos de TIC deve ser realizada periodicamente para garantir seu bom funcionamento e prolongar sua vida útil.

6.2. É vedado aos usuários realizar qualquer alteração na configuração de hardware dos ativos de TI sem autorização prévia da GERSOL. Em caso de falha ou mau funcionamento de qualquer dispositivo de TI, é obrigatório acionar o suporte técnico adequado para as devidas correções.

6.3. Qualquer problema ou falha em ativos de TIC deve ser reportado imediatamente por meio de abertura de chamado técnico, para que ações corretivas sejam tomadas rapidamente.

7. SEGURANÇA DE ATIVOS

7.1. Todos os ativos de TIC devem ser protegidos contra acessos não autorizados, perda, roubo, danos físicos e cibernéticos.

7.2. Medidas de segurança, como criptografia, backups regulares, controle de acesso e antivírus, devem ser implementadas e mantidas atualizadas.

8. DESCARTE DE ATIVOS

8.1. O descarte de ativos de TIC deve ser realizado de maneira segura e ambientalmente responsável, em conformidade com as regulamentações aplicáveis.

8.2. Antes do descarte, todos os dados e informações contidas nos ativos de TIC devem ser excluídos de forma irreversível e segura, compatível com a sua classificação de segurança.

9. DOCUMENTOS RELACIONADOS

9.1. Política de Segurança da Informação (9520132).

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br

PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

ANEXO V

Rio de Janeiro, 18 de março de 2025.

TERMO DE SIGILO E CONFIDENCIALIDADE

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

Este Termo de Sigilo e Confidencialidade destina-se aos empregados terceirizados que, em razão de suas atividades, tenham acesso direto ou indireto a informações sensíveis, confidenciais ou estratégicas, estabelecendo as responsabilidades e obrigações desses colaboradores quanto à proteção e preservação da confidencialidade das informações da PortosRio.

Processo SEI nº	
Contrato nº	
Empresa:	
Objeto:	

Eu, (nome do representante da empresa), abaixo assinado, portador do documento de identidade nº XXXXXXX, expedido por XXXXXXX, e do CPF nº XXXXXXX <O número de identificação da identidade e CPF devem ficar parcialmente suprimidos. Exemplo: CPF nº 999.xxx.999.xx>, prestador de serviços da empresa (nome da empresa), no exercício de minhas atividades, declaro que estou plenamente ciente das obrigações e responsabilidades que assumo ao acessar, manusear, utilizar e divulgar informações confidenciais e sigilosas pertencentes à empresa.

Comprometo-me a:

I - Manter absoluto sigilo sobre quaisquer informações confidenciais e/ou sensíveis da PortosRio às quais eu tenha acesso, direta ou indiretamente, durante e após o término do meu vínculo com a empresa.

II - Utilizar as informações confidenciais exclusivamente para fins relacionados às minhas funções na PortosRio, abstendo-me de utilizar tais informações para qualquer benefício pessoal ou de terceiros.

III - Não divulgar, repassar ou compartilhar informações confidenciais com quaisquer pessoas, dentro ou fora da empresa, que não estejam autorizadas a acessá-las.

IV - Adotar todas as medidas necessárias para proteger as informações confidenciais contra acessos não autorizados, perdas, roubos, danos ou qualquer forma de exposição inadequada.

V - Devolver todos os documentos, materiais e quaisquer outros meios contendo informações confidenciais à PortosRio, imediatamente após o término do meu vínculo empregatício ou a qualquer momento quando solicitado pela empresa.

VI - Reconhecer que a violação das obrigações de confidencialidade pode resultar em medidas disciplinares, ações legais e a obrigação de indenizar a empresa por quaisquer danos causados.

Para os fins deste termo, consideram-se **informações confidenciais** quaisquer dados, documentos, materiais, estratégias, planos, projetos, processos, tecnologias, know-how, contratos, acordos, informações financeiras, comerciais, operacionais e quaisquer outras informações que não sejam de domínio público e que sejam consideradas sigilosas pela empresa.

Este termo tem validade durante o período em que eu estiver vinculado à empresa e perdurará mesmo após o término desse vínculo ou enquanto as informações mantiverem seu caráter confidencial.

Ao assinar este termo, declaro ter lido, compreendido e aceitado integralmente as condições aqui estabelecidas, comprometendo-me a cumpri-las rigorosamente.

NOME DO REPRESENTANTE
Nome da Empresa

NOME DO GESTOR DO CONTRATO
Registro Funcional

NOME DO FISCAL DO CONTRATO
Registro Funcional

1. DOCUMENTOS RELACIONADOS

1.1. Política de Segurança da Informação (9520132).

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br