Diretrizes para Desenvolvimento Seguro			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
52-DDS	2.1	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
A.14.2 da 27001		11/06/2024	1/4

SUMÁRIO

1 OBJETIVO

Este documento tem por objetivo apresentar as diretrizes para o desenvolvimento seguro de software no ambiente do LNCC, contemplando recomendações de boas práticas para o desenvolvimento e manutenção de softwares, incluindo scripts de automação de tarefas, utilizados de forma regular para atender as necessidades das áreas de atuação do LNCC.

2 CAMPO DE APLICAÇÃO

As diretrizes apontadas neste documento aplicam-se ao desenvolvimento de software, no desenvolvimento de soluções que atuam nos ativos do Supercomputador Santos Dumont (SSD) e nos ativos da instituição hospedados no datacenter.

3 RESPONSABILIDADE

A responsabilidade pela elaboração, análise crítica, publicação ou cancelamento desta norma é do SERED. A responsabilidade pela aprovação desta norma é da Comitê de Privacidade e Segurança da Informação (CPSI). O Gestor de Segurança da Informação (GSI) e o CPSI devem apoiar o processo de elaboração e análise crítica deste documento.

4 DOCUMENTOS DE REFERÊNCIA

Os documentos a seguir, no todo ou em parte, são referenciados neste documento e fornecem requisitos, diretrizes ou orientações que são indispensáveis à sua aplicação. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do documento, incluindo emendas.

ISO/IEC 27000:2018	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ABNT NBR ISO/IEC 27001:2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação
Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Glossário de Segurança da Informação
Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020	Dispõe sobre a estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal

5 DOCUMENTOS COMPLEMENTARES

Os documentos a seguir serão utilizados, no todo ou em parte, para viabilizar a aplicação das informações documentadas do SGSI, devendo estar citados no corpo do texto normativo e disponíveis para uso.

11-PS	Política de Senhas LNCC

6 SIGLAS

API Interface de Programação de Aplicação, do inglês *Application Programming Interface*
COTIC Coordenação de Tecnologia da Informação e Comunicação
CSIC Comitê de Segurança da Informação e Comunicações e de Segurança Física
DDoS Ataque de Negação de Serviço Distribuído, do inglês *Distributed Denial of Service*
LNCC Laboratório Nacional de Computação Científica
SGSI Sistema de Gestão de Segurança da Informação

SQL Linguagem de Consulta Estruturada, do inglês *Structured Query Language*
SSD Supercomputador Santos Dumont

7 TERMOS E DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência, Portaria GSI/PR nº 93/2021 e ISO/IEC 27000:2018, que devem ser interpretados somando-se as descrições. Em caso de divergência, prevalecem o termo e a definição estabelecidos na Portaria GSI/PR nº 93/2021.

VULNERABILIDADE	Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.
PRINCÍPIO DO PRIVILÉGIO MÍNIMO	Princípio do privilégio mínimo, do inglês *Principle Of Least Privilege* (POLP) consiste em limitar os direitos de acesso dos usuários ao que é estritamente necessário para realizar suas atividades.
INTEGRIDADE	Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
FRAMEWORK	Conjunto básico de classes, interfaces e componentes que funcionam de forma integrada e servem de base para construção de sistemas

8 DIRETRIZES

8.1 Recomenda-se que sejam utilizados meios de armazenamento que possuam controle de acesso. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os meios de armazenamento devem possuir controle de acesso de forma que seja possível gerenciar, no mínimo, as permissões de leitura, edição e execução dos arquivos.

ii. As permissões dos sistemas de armazenamento devem ser configuradas com o princípio do menor privilégio.

8.2 Recomenda-se que seja empregado canal de comunicação que forneça controle de integridade dos dados transmitidos. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Toda comunicação realizada entre os sistemas deve implementar controles que garantam a integridade de toda informação enviada e recebida.

8.3 Recomenda-se documentar as medidas protetivas aplicadas ao código-fonte. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Toda medida protetiva implementada para mitigação de vulnerabilidade ou correção de falha de segurança deve ser registrada e documentada.

8.4 Recomenda-se utilizar controles de usuário e senha nominais para determinar a identidade de cada usuário. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os softwares desenvolvidos devem implementar o controle de acesso por meio de usuário e senha, de forma que seja possível diferenciar cada usuário que o utiliza.

ii. Usuários genéricos devem ser evitados.

8.5 Recomenda-se manter o controle das mudanças realizadas em sistemas, preferencialmente, com apoio de ferramenta para controle de versão de todo código criado ou atualizado. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Toda alteração de código-fonte deve ser controlada por meio de procedimento específico.

ii. Os softwares devem possuir controle de versão, preferencialmente, através de ferramenta automatizada que permita a recuperação de um estado anterior do código-fonte e consulta ao histórico de versões.

Nota: São exemplos de ferramentas para esta finalidade: cvs, svn, git, entre outras.

8.6 Não se recomenda habilitar atualizações automáticas de bibliotecas e componentes utilizados. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. As atualizações de bibliotecas e componentes utilizados no desenvolvimento dos sistemas deve ser devidamente controlada através de procedimentos de testes e validações específicos.

8.7 Não se recomenda utilizar bibliotecas e frameworks obsoletos e sem suporte para correções e atualizações de segurança. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os conjuntos de bibliotecas e de frameworks devem ser cuidadosamente selecionados de forma que todos os componentes dos sistemas desenvolvidos sejam compatíveis entre si e possuam suporte para correções e atualizações de segurança.

8.8 Não se recomenda realizar o acesso a aplicações de banco de dados utilizando login de usuário com permissões de root/administrador. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. O acesso às aplicações de banco de dados deve ser realizado por meio de conta específica, cujas permissões devem ser configuradas com o princípio do menor privilégio.

8.9 Recomenda-se a elaboração de senhas que sigam os padrões estabelecidos na política de senhas do LNCC, estabelecida no documento 11-PS. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os sistemas desenvolvidos devem implementar a política de senhas do LNCC ou fazer uso de algum serviço de autenticação que a implemente.

8.10 Não se recomenda armazenar senhas em texto claro ou de forma insegura. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. As senhas de acesso a bancos de dados, API's ou qualquer outro serviço, que os sistemas necessitem se conectar, não devem ser armazenadas em texto claro, seja dentro do código-fonte ou em arquivos de configuração adicionais.

ii. Devem ser utilizadas técnicas que garantam a segurança dessas conexões.

8.11 Recomenda-se que as aplicações produzam registro de log das ações. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os sistemas devem produzir registros das ações de forma que seja possível realizar auditorias no uso dos sistemas.

ii. Os registros devem ser armazenados em arquivos adicionais, bancos de dados ou através do serviço de logs do sistema operacional.

iii. Os registros de erro não devem revelar detalhes da sua estrutura interna do software.

8.12 Recomenda-se que o código-fonte seja revisado regularmente. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. A revisão do código deve ser realizada por pares, ou seja, o revisor deve ser uma pessoa diferente da pessoa responsável pelo desenvolvimento do código.

ii. A revisão deve buscar identificar problemas em um estágio inicial, antes do código ser integrado ao sistema principal.

8.13 Recomenda-se que os softwares e sistemas desenvolvidos sejam analisandos quanto a existência de vulnerabilidades de segurança. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Todo software desenvolvido deve ser analisado quanto à existência de vulnerabilidades de segurança, principalmente quanto à injeção de código SQL, à injeção de comandos, à falta de controle de acesso, à falta de validação de entrada de dados, a não criptografia de dados sensíveis e a não proteção contra-ataques de negação de serviço DDoS.

8.14 Recomenda-se que haja um monitoramento e acompanhamento das tratativas para as vulnerabilidades encontradas. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Deve ser mantido o registro das vulnerabilidades encontradas nos sistemas, assim como todo o processo de tratativa para mitigação das vulnerabilidades, contemplando aplicação de patches, atualização de bibliotecas, correções de código-fonte etc.

8.15 Recomenda-se que todo software ou sistema desenvolvido permita o gerenciamento e controle de acesso dos usuários. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os softwares desenvolvidos no âmbito do LNCC, sempre que possível, devem implementar mecanismos que permitam o controle de acesso aos usuários conforme demais recomendações desta norma.

8.16 Recomenda-se a utilização de testes de segurança automatizados para acelerar o processo de detecção de erros, bugs e vulnerabilidades. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Devem ser implementados os testes de software através de ferramentas automatizadas visando facilitar e agilizar a etapa de testes, sempre que possível.

8.17 Recomenda-se que todo código seja testado em ambiente controlado antes de ser incluído em ambiente de produção. Caso a recomendação seja aplicada, deve ser seguido o disposto:

i. Os testes de código-fonte devem ser realizados em ambiente controlado. Esse ambiente deve ser capaz de reproduzir as particularidades do ambiente de produção, dessa forma espera-se que todas as funcionalidades implementadas possam ser validadas.

9 MANUTENÇÃO DO DOCUMENTO

9.1 Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, ao menos, uma vez ao ano.

10 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	23/05/2023	Documento Inicial.
1.1	19/03/2024	Correções no texto.
2.0	28/05/2024	Revisão do texto e remoção da seção “diretrizes gerais”.
2.1	11/06/2024	Reclassificação do nível de acesso Interno para Externo.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por	Bruno Alves Fagundes	Chefe do SERED
Verificado por	Luis Rodrigo de Oliveira Gonçalves	Gestor de segurança da informação
Aprovado por	Wagner Vieira Léo	Coordenador da COTIC

Documento assinado eletronicamente no Processo SEI nº 01209.000061/2020-55.

_____