GETII/COBAN

CÓDIGO	TÍTULO	VIGÊNCIA	VERSÃO
NORMA 002/2024	NORMA DE ACESSO BANCO DE DADOS	11/11/2024	1

1 PREFÁCIO

A presente Norma está de acordo com as diretrizes da Política de Segurança da Informação e Comunicação do CIASC.

2 OBJETIVO

O objetivo deste documento é normatizar o acesso aos Bancos de Dados administrados e gerenciados pelo CIASC.

3 ESCOPO

Esta norma se aplica a todos os usuários (clientes, prestadores de serviços, parceiros, estagiários, bolsistas e empregados) que utilizam o ambiente do CIASC para acesso a serviços internos na Rede de Governo.

4 TERMOS E DEFINIÇÕES

Para efeito desta Norma aplicam-se os seguintes conceitos e definições:

Segurança da Informação e Comunicação (SIC) – proteção da informação contra ameaças para garantir a continuidade das atividades finalísticas e meio da instituição, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no CIASC.

Incidente em Segurança da Informação – qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações da instituição ou ameaçar a segurança da informação.

Usuário – qualquer pessoa (empregados, clientes, visitantes, estagiários, empregados temporários, prestadores de serviços, colaboradores...) que possuam ou não ligação com o CIASC, e que necessitem de acesso a um sistema ou recurso computacional do CIASC.

Cadeia de Custódia - no contexto legal, refere-se à documentação cronológica ou histórica que registra a sequência de custódia, controle, transferência, análise e disposição de evidências físicas ou eletrônicas.

SGBD - Data Base Management System ou Sistema de Gerenciamento de Banco de Dados é um conjunto de software utilizado para o gerenciamento de uma base de dados, responsável por controlar, acessar, organizar e proteger as informações de uma aplicação, tendo como principal objetivo gerenciar as bases de dados utilizadas.

Gestor - Gerente da Área ou pessoa delegada indicada formalmente para gerenciar o acesso às informações.

5 Papéis e Responsabilidades

5.1 Usuário

- Manter sigilo das informações de acesso ao ambiente de rede do CIASC e da conexão remota, sendo de sua total e exclusiva responsabilidade, qualquer operação realizada por meio de suas credenciais de acesso;
- Comunicar imediatamente à área de Segurança da Informação (COSEI) qualquer situação que coloque em risco o acesso ao ambiente da rede de dados do CIASC; e

- Informar seu gestor quando forem identificados direitos de acesso remoto desnecessários à execução dessas atividades.

5.2 Gestor

- Solicitar e/ou revogar as credenciais de acesso dos usuários sob sua gestão;
- Conscientizar os usuários em seu domínio administrativo, quanto às orientações presentes neste documento e nas boas práticas de segurança;
- Comunicar imediatamente ao setor de Segurança da Informação (COSEI) caso verifique qualquer ameaça, vulnerabilidade ou situação que possa colocar em risco o ambiente computacional em questão; e
- Manter atualizada relação de usuários e seus papéis para que, de forma contínua, seja verificada a política de acessos mínimos e com isso a adequação dos perfis de acesso dos respectivos usuários.

5.3 Gerência de *Data Center* (GETII)

- Administrar os acessos remotos ao ambiente de banco de dados do CIASC;
- Monitorar todo o ambiente de modo a identificar, proativamente, anomalias e acessos maliciosos;
- Efetuar auditorias no ambiente como forma de garantir que os mecanismos de segurança adotados se mantêm eficientes.
- Prover os mecanismos de auditoria apontados pelos desenvolvedores ou o próprio cliente, dono da base de dados.

5.4 Gerência de Redes (GERED)

- Monitorar todo o ambiente de modo a identificar, proativamente, anomalias e acessos maliciosos;

- Manter mecanismos de segregação de acesso lógico entre os ambientes de acesso remoto e os recursos computacionais em ambiente de rede local controlando o acesso por meio de políticas de acessos mínimos;

5.5 Gerência de Recursos Humanos (GEPES)

- Notificar à equipe da GETII/COBAN e GETII/COAPE para revogação de credenciais de acesso remoto de funcionários que entrarem em licenças sem vencimento, desligamento definitivo, desligamento temporário por decisão judicial, afastamentos por licença de saúde ou que forem colocados à disposição de outros órgãos; e
- Conscientizar os novos funcionários quanto às orientações presentes neste documento e nas boas práticas de segurança.

6 DIRETRIZES

6.1 Ambientes

6.1.1 Bases de produção

6.1.1.1 O acesso deve ser restrito a apenas sistemas e DBAs

6.1.2 Bases de testes e homologação

6.1.2.1 Para uso de terceirizados, dados pessoais devem ser anonimizados.

6.2 Privilégio Mínimo

6.2.1 Devem ser concedidos apenas os acessos necessários para o desenvolvimento de sistemas.

6.2.2 Cada sistema deve possuir seu próprio usuário de acesso aos dados.

6.2.3 Não devem ser utilizados usuários com perfil de DBA ou administrador nos acessos a sistemas.

6.3 Segurança dos Dados

6.3.1 As conexões devem utilizar criptografia por meio de protocolos seguros.

6.3.2 Os dados em repouso devem utilizar criptografia de disco ou nativa do SGBD.

6.3.3 Toda base deve conter backup.

6.4 Auditoria dos acessos

6.4.1 **T**oda base de dados deve ter um mecanismo de auditoria para que sejam apurados acessos indevidos (logs de acessos).

6.4.2 Deve ser possível a identificação da origem de ip, usuário e comando.

6.5 Acessos Diretos ao Banco de dados

6.5.1 Acessos realizados diretamente pelos clientes devem ser alertados dos riscos e estes devem providenciar assinatura de termo para autorização do acesso.

6.5.2 Acessos que possam quebrar a cadeia de custódia dos dados devem conter autorização e assinatura do cliente.

6.6 Compartilhamento de Dados

6.6.1 Compartilhamentos de dados entre órgãos distintos devem ter a autorização do órgão dono da base de dados por meio do termo de compartilhamento de dados assinado pelo cliente.

6.6.2 A documentação sobre compartilhamentos deve ser disponibilizada no sistema de gestão de projetos (Jira).

6.7 Cópia de Base de Dados

6.7.1 O cliente deve ser alertado dos riscos quando este solicitar cópia de base de dados, a entrega deve ser providenciada em meio de compartilhamento de arquivo seguro, temporário e restrito, devendo o cliente assinar termo de recebimento.

6.7.2 Cópia de base de dados de produção para pré-produção ou homologação, quando necessária, deverá conter as mesmas permissões do ambiente de produção. As liberações adicionais devem ser realizadas em modo de exceção. Dados sensíveis devem ser anonimizados.

6.8 Exceções

6.8.1 A equipe da COBAN deverá administrar eventuais exceções que vierem a ocorrer.

6.8.2 Na sua ausência do gestor, devem ser autorizadas pelo gerente da GETII.

7 SANÇÕES

A violação desta política por qualquer usuário será reportada ao CGSI - Comitê Gestor de Segurança da Informação do CIASC e ao superior imediato que liberou o acesso e que

poderá tomar medidas para suspender de forma imediata, temporária ou permanente os seus privilégios de acesso a rede local de dados, bem como encaminhar os fatos às áreas pertinentes para aplicação das medidas administrativas cabíveis com vistas a impor as sanções aplicáveis, seja no âmbito de responsabilização interna, através de sanções disciplinares, seja no âmbito externo, às pessoas físicas ou jurídicas, tais como multas e demais sanções previstas em contratos, respeitado o princípio da proporcionalidade e do devido processo legal, sem prejuízo de eventual ação judicial para reparação dos danos e preservação dos direitos desta empresa.

8 Referências Bibliográficas

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de segurança - Código de prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2013.

9 Histórico de versões

Alterações	Data de aprovação	Versão gerada
Primeira versão	24/10/2024	v1