LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA
Av. Getúlio Vargas, nº 333, - Bairro Quitandinha,
CEP 25651-075, Petrópolis - RJ - http://www.lncc.br

Plano de Emergências			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
40-PE	4.1	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022			**PUBLICADO EM**
A.5.24; A.5.25; A.5.26; A.5.27; A.5.28; A.6.8.			18/11/2025

SUMÁRIO

Objetivo
Campo de aplicação
Responsabilidade
Documentos de referência
Documentos complementares
Termos e definições
Siglas
Responsabilidades e procedimentos
Orientações para atuação
Orientações para medidas de prevenção
Divulgação, conscientização e monitoramento
Encerramento e aprendizado com incidentes
Retorno ao colaborador
Histórico da revisão e Quadro de aprovação
ANEXOS

1. OBJETIVO

Este documento baseia-se nas seções sobre gestão de incidentes de segurança da informação da norma ABNT NBR ISO/IEC 27001 e apresenta o Plano de Emergências do LNCC.

O objetivo deste Plano é padronizar as medidas a serem adotadas para prevenir eventos de emergências que envolvam risco à vida ou ao patrimônio da organização, assim como as medidas a serem adotadas na tratativa de eventuais emergências, incluindo ações em casos de acidente, incêndio ou mal súbito ocorridos nas dependências do LNCC.

Além da padronização, este documento visa determinar como deve ocorrer o processo de divulgação das informações nele contidas.

2. CAMPO DE APLICAÇÃO

Este Plano é aplicável a todo o ambiente do campus do LNCC ou outro ambiente que esteja sob a sua responsabilidade. Da mesma forma, ele é aplicável a todos os colaboradores da instituição, incluindo visitantes.

Este Plano deve ser de conhecimento de todos os colaboradores da instituição. Sendo que os controles relacionados à proteção da vida também devem ser de conhecimento de eventuais visitantes e equipes externas que venham realizar alguma atividade.

Periodicamente os colaboradores devem ser informados acerca da necessidade e importância da execução das ações relacionadas a este plano.

3. RESPONSABILIDADE

A chefia do SECAM é a responsável pela elaboração e pela análise crítica deste documento. A responsabilidade pela sua aprovação e pelo seu cancelamento é da Coordenação da COGEA. O Gestor de Segurança da Informação é o responsável pela publicação 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.

ABNT NBR ISO/IEC 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Aprova o Glossário de Segurança da Informação (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370)
Portaria MCTI nº 7.061, de 24 de maio de 2023	Aprova o Regimento Interno do Laboratório Nacional de Computação Científica (https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159)

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.

02-PSI	Política de Segurança da Informação do LNCC.
03-PSISD	Política de Segurança da Informação – LNCC / Santos Dumont.

6. TERMOS E DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os termos e definições 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.

Agente público	Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, um mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta.
Colaborador	Qualquer agente público, aluno, bolsista, estagiário, menor aprendiz, terceirizado ou indivíduo que direta ou indiretamente utiliza ou suporta a pesquisa, os processos, sistemas, infraestrutura ou informações da instituição.

7. SIGLAS

LNCC Laboratório Nacional de Computação Científica

SGSI Sistema de Gestão de Segurança da Informação

CPSIC Comitê de Privacidade e Segurança da Informação, Comunicações e de Segurança Física

CBMERJ Corpo de Bombeiros Militar do Estado do Rio de Janeiro

Nota: As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica (https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159).

8. RESPONSABILIDADES E PROCEDIMENTOS

8.1 Em caso de ameaça concreta à vida ou ao patrimônio da instituição, os colaboradores devem realizar a comunicação imediata do incidente à Equipe de Vigilância Patrimonial, que deverá avaliar e comunicar diretamente aos contatos listados abaixo:

Tabela 1 – Contatos para resolução de emergências

EMERGÊNCIA	QUEM	CONTATO
TODAS – INFORMAR	SECAM (2ª a 6ª, 8h às 17h)	Ramais: 6034, 6201 ou 6127. E-mail: secam@lncc.br
	Equipe de Vigilância Patrimonial (17h às 8h e finais de semana)	Portaria do LNCC – ramal: 6262. Sala da Vigilância (1C12) – ramal: 6207.
Incêndio ou acidentes com pessoas envolvidas em: soterramento, exposição a gases, químicos etc.	Quartel do CBMERJ em Petrópolis	193 ou (24) 2291-0928
Colaborador passando mal, demandando atendimento de emergência	Serviço de Atendimento Móvel de Urgência – SAMU	192 ou (24) 2244-4150

Atendimentos médicos de Urgência e Emergência	Hospital Municipal Dr. Nelson Sá Earp – Urgências ortopédicas e psiquiátricas	Rua Paulino Afonso, 455 – Bingen – (24) 2237-4062
	UPA Centro – Urgências clínicas, pediátricas e odontológicas	Rua Washington Luiz, 600 – Centro – (24) 2246-9132
Atendimentos médicos de Urgência e Emergência	Pronto Socorro Leônidas Sampaio – Urgências clínicas	Rua Teresa, 1839 – Alto da Serra – (24) 2231-5566
	UPA Cascatinha – Situações de picadas de animais peçonhentos e mordeduras caninas	Rua Bernardo Proença, 500 – Cascatinha – (24) 2246-8931
Desastre natural alcançando as instalações do LNCC	Defesa Civil de Petrópolis	199 ou (24) 2242-9281
Falta de energia elétrica	ENEL – concessionária de energia elétrica	0800 28 00 120
Falta de água	Águas do Imperador	0800 742 0422

8.1.1 Em todos os casos, independente das ações que possam ser tomadas pelo colaborador, compete ao mesmo informar ao SECAM durante o horário de expediente diurno e à Equipe de Vigilância Patrimonial nos demais horários, para que seja adotada ação para mitigação da ameaça, orientação aos colaboradores e comunicação aos órgãos de segurança pública – Polícias, Defesa Civil, Corpo de Bombeiros ou SAMU.

8.2 Comunicação de incidentes de segurança da informação

8.2.1 Os colaboradores devem comunicar imediatamente quaisquer eventos de segurança da informação observados ou suspeitos aos canais definidos neste plano. Incluindo incidentes observados por terceiros, suspeitas ou tentativas fracassadas de ataque.

8.2.2 São exemplos de incidentes que devem ser comunicados:

a) acessos não autorizados a sistemas, informações ou áreas restritas;

b) vazamento ou perda de informações confidenciais;

c) falhas de software ou hardware que comprometam a segurança;

d) tentativas de phishing ou engenharia social;

e) infecção por malware ou comportamento anômalo em sistemas;

f) utilização indevida de credenciais ou senhas;

g) envio acidental de informações sensíveis a destinatários incorretos.

8.2.3 O colaborador não deve tentar testar, explorar ou investigar vulnerabilidades por conta própria, devendo sempre acionar o ETIR.

8.3 Classificação e priorização de incidentes

8.3.1 Os incidentes de segurança da informação relatados serão avaliados com base em critérios como:

a) impacto potencial à confidencialidade, integridade e disponibilidade da informação;

b) escopo afetado (local, institucional, externo);

c) sensibilidade dos dados envolvidos;

d) urgência da resposta necessária.

8.3.2 O registro formal da avaliação será realizado por meio de formulário próprio e armazenado para rastreabilidade e análise futura.

9. ORIENTAÇÕES PARA ATUAÇÃO

9.1 Incêndio e acidentes com pessoas

9.1.1 Casos de incêndio, vazamentos de gás, salvamentos de pessoas ou animais, retiradas de animais silvestres ou que representem um risco, soterramentos, acidentes envolvendo produtos químicos e queimadas devem ser comunicados ao SECAM ou à Equipe de Vigilância Patrimonial, para orientação aos colaboradores e acionamento do CBMERJ.

9.1.2 Somente colaboradores qualificados em prestação de socorros ou em combate a incêndios devem atuar no socorro ou no combate ao fogo.

9.1.3 Na ocorrência de incêndio, os colaboradores devem usar do caminho de saída mais rápido e dirigirem-se ao local de encontro em caso de emergência, conforme plantas a serem afixadas em corredores próximos às escadas (plantas anexas).

9.2 Emergência médica

9.2.1 Em caso de emergências médicas, prestar os primeiros socorros e, em caso de necessidade de remoção, informar ao SECAM ou à Equipe de Vigilância Patrimonial e acionar o SAMU (pronto-socorro).

9.2.2 Somente colaboradores qualificados em prestação de socorros devem atuar no socorro às pessoas em situação de emergência médica, mesmo se for avaliada a necessidade de remoção por meio de veículo próprio. Neste caso, dever-se-á dirigir-se à unidade mais próxima de atendimentos médicos de Urgência e Emergência ou ainda à emergência de rede particular à qual o colaborador se encontre filiado.

9.3 Eventos de Defesa Civil – temporais, inundações, desmoronamentos e incêndios florestais

9.3.1 A Defesa Civil é responsável por prevenir, socorrer, assistir e ajudar na recuperação da população em caso de desastres naturais, sejam: chuvas, inundação, queda de arvore, vendaval, deslizamentos, alagamentos ou outras situações de risco.

9.3.2 O colaborador deve informar o evento ao SECAM ou à Equipe de Vigilância Patrimonial, que comunicará à Defesa Civil.

9.4 Falta de energia

9.4.1 Em caso de falha do fornecimento de energia elétrica, o sistema estabilizado (no qual são ligados os computadores) e alguns pontos de iluminação permanecerão funcionando por meio de gerador a diesel por período de cerca de

3 h. Antes de se completarem as 3 horas e de forma a evitar a penumbra na sala, corredores e escadas, compete ao colaborador desligar seu computador, fechar a sala e retornar ao seu domicílio.

9.4.2 Em caso de falha do fornecimento de energia elétrica diurnamente comunicar ao SECAM, ou à noite à Equipe de Vigilância Patrimonial.

9.5 Falta d'água

9.5.1 Em caso de falta d'água, diurnamente comunicar ao SECAM ou à noite à Equipe de Vigilância Patrimonial.

9.6 Incidentes de segurança da informação

9.6.1 Em caso de incidente de segurança da informação:

a) o colaborador deve comunicar imediatamente a ETIR;

b) o sistema afetado deve ser isolado sempre que possível, evitando desligamentos que comprometam evidências;

c) devem ser preservadas as evidências digitais (arquivos de log, registros de acesso, prints de tela etc.) com apoio da equipe técnica;

d) todas as ações realizadas durante a resposta ao incidente devem ser registradas em relatório próprio. Esse registro deverá conter data, hora, responsável, ação executada e observações.

9.6.2 Quando necessário, poderá ser realizada análise forense ou perícia técnica para aprofundamento da investigação. As evidências coletadas deverão ser mantidas conforme práticas de cadeia de custódia para eventual uso jurídico, disciplinar ou auditoria.

9.6.3 A coleta de evidências digitais deverá seguir processo documentado que garanta:

a) identificação da origem, tipo e formato das evidências;

b) registro da cadeia de custódia, com responsáveis e datas;

c) proteção contra alteração ou corrupção de dados;

d) armazenamento seguro dos registros digitais;

e) aderência à legislação aplicável.

10. ORIENTAÇÕES PARA MEDIDAS DE PREVENÇÃO

10.1 Todo colaborador é responsável pela manutenção de um ambiente físico e social livre de riscos à saúde, à segurança humana, à proteção do meio ambiente e à segurança patrimonial.

10.2 Contribuições de aperfeiçoamento devem ser feitas à equipe do SECAM.

10.3 Incidentes relacionados aos circuitos elétricos

10.3.1 Em face de que as tomadas compõem um circuito elétrico cuja capacidade de uso foi dimensionada de forma coletiva, envolvendo diâmetro da fiação e capacidade de corte de disjuntores por áreas, não por sala, o colaborador é o principal responsável pelo uso da rede elétrica sem riscos, obedecendo às seguintes normas:

i) não conectar equipamentos estranhos à rede elétrica estabilizada, que deve ser utilizada apenas para equipamentos de informática;

ii) não conectar equipamentos de alta potência, tais como fornos de resistência elétrica ou micro-ondas, sanduicheiras, torradeiras, cafeteiras, aquecedores etc.

sem a autorização do SECAM, que verificará a capacidade elétrica da rede que abastece à sala;

iii) à noite, nos finais de semana, nos períodos de férias, feriados prolongados e outros períodos nos quais os colaboradores fiquem ausentes das salas, recomenda-se que o colaborador desconecte todos os equipamentos das tomadas elétricas ou desligue réguas, quando for o caso;

iv) não manter líquidos sobre mesas, os quais, em caso de derramamento, podem atingir equipamentos elétricos e causar curtos-circuitos;

v) não deixar janelas abertas quando da ausência do colaborador, pois temporais também podem causar inundação ou vir a molhar tomadas, causar curtos-circuitos e provocar incêndios;

vi) observar, sempre que possível, se há aquecimento de tomadas e plugues, que são sinal de mau contato e podem indicar princípio de incêndio;

vii) em todos os casos de suspeita de defeito elétrico, o colaborador deve entrar em contato com o SECAM.

Nota: As tomadas elétricas conectadas à rede estabilizada geralmente estão sinalizadas na cor vermelha, utilizam o padrão ABNT antigo e possuem suporte a 3 pinos; já as tomadas conectadas a rede elétrica não estabilizada estão sinalizadas nas cores cinza ou preta, utilizam padrão ABNT antigo com suporte a 2 pinos.

10.4 Segurança e manutenção das salas

10.4.1 O colaborador deve garantir que:

i) a sala fique fechada assim como as janelas, quando for se ausentar por longo período, evitando a entrada de animais e a inundação por temporais;

ii) a limpeza de janelas seja feita apenas por pessoal da equipe de limpeza;

iii) para as salas do segundo andar, o colaborador deve assegurar que não haja planta ou equipamento que possa despencar de móvel próximo ou do peitoril da janela e causar danos à saúde humana ou ao patrimônio – quebra de vidro da janela da sala debaixo;

iv) não usar das lixeiras de escritório para a disposição de restos de alimentos, pois estes, certamente, atrairão insetos e outras pragas para aquele ambiente.

10.4.2 O colaborador deve ter em mente que o patrimônio da União sob seu uso está, para todos os efeitos, sob sua responsabilidade administrativa.

11. DIVULGAÇÃO, CONSCIENTIZAÇÃO E MONITORAMENTO

11.1 Os contatos telefônicos, os endereços de e-mail, as rotas de fuga e as recomendações apresentadas neste documento devem ser fixadas nas salas utilizadas pelos colaboradores e nas áreas públicas, tais como corredores, auditórios e biblioteca.

11.2 A sinalização da “SAÍDA” acompanhada de seta deve ser fixada nos corredores e áreas públicas para indicar rota de fuga.

11.3 As informações contidas neste documento devem fazer parte das campanhas e treinamentos de segurança da informação. Periodicamente, os colaboradores devem ser lembrados quanto às orientações apresentadas neste documento.

11.4 A divulgação do Plano de Emergências deve ser periodicamente efetuada, de forma a que todos os colaboradores sejam mantidos alertas para a prevenção e combate de incêndios e demais eventos. Além dos colaboradores, os visitantes e

participantes de eventos devem ter conhecimento do conteúdo deste documento.

11.5 As medidas contidas neste documento devem ser divulgadas em todos os eventos que ocorrerem nas dependências do LNCC.

12. ENCERRAMENTO E APRENDIZADO COM INCIDENTES

12.1 Após a resolução de um incidente relevante, deverá ser elaborado um relatório final com:

a) descrição detalhada do evento;

b) causas identificadas e ações tomadas;

c) impacto e consequências;

d) lições aprendidas e oportunidades de melhoria.

12.2 Esses relatórios servirão de base para revisões periódicas do plano, ações de capacitação e atualizações nos controles do SGSI.

12.3 As lições aprendidas serão incorporadas em futuras campanhas de conscientização, promovendo a prevenção de incidentes similares. Os resultados também devem ser apresentados ao CPSIC, quando pertinente, para avaliação estratégica e integração com planos de ação.

13. RETORNO AO COLABORADOR

13.1 Sempre que possível, será fornecido retorno ao colaborador que reportou o incidente, informando, de forma sintética e respeitando a confidencialidade, as providências adotadas.

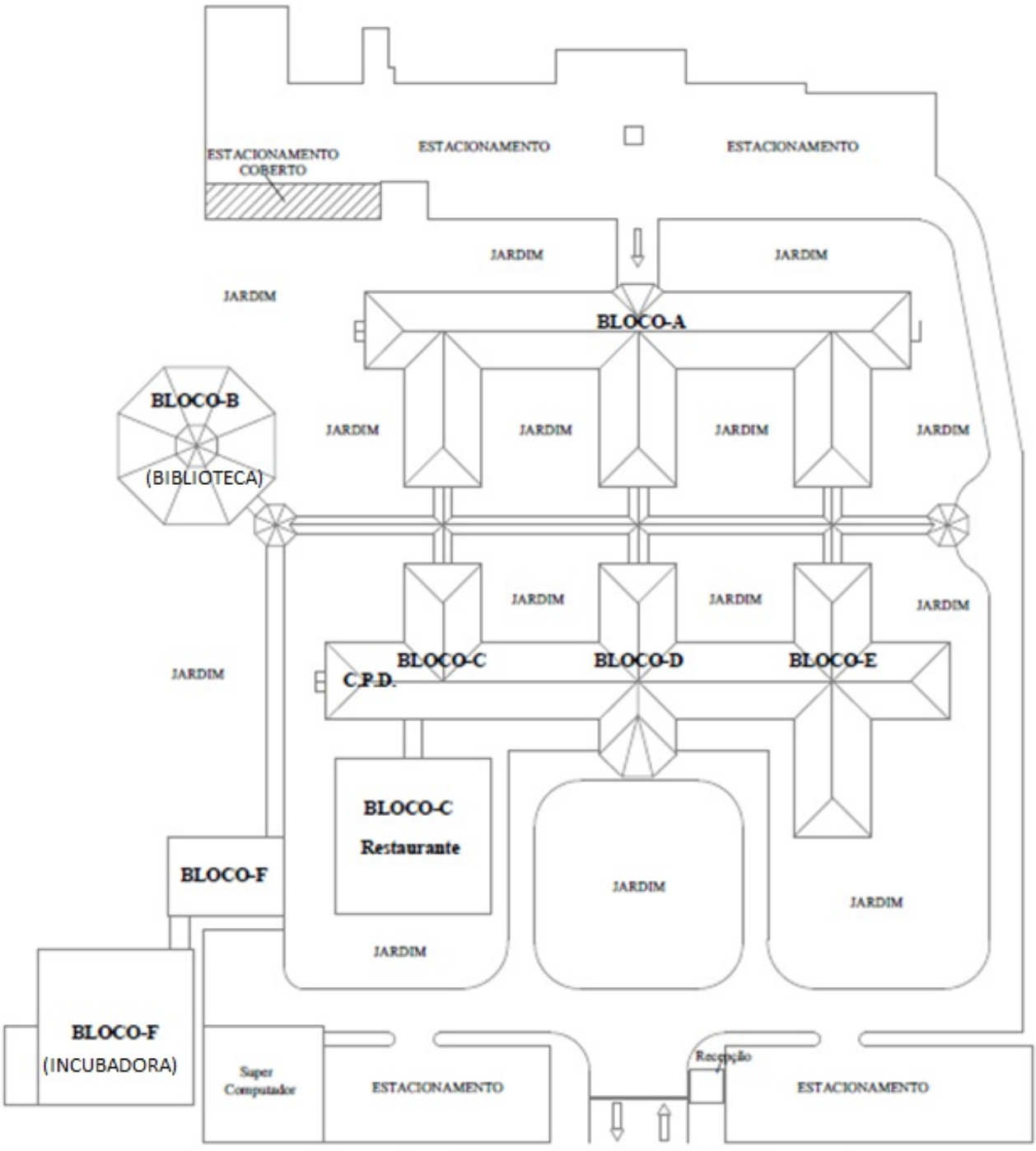
13.2 Esse processo visa incentivar o reporte e garantir transparência e confiança na gestão de incidentes.

14. HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

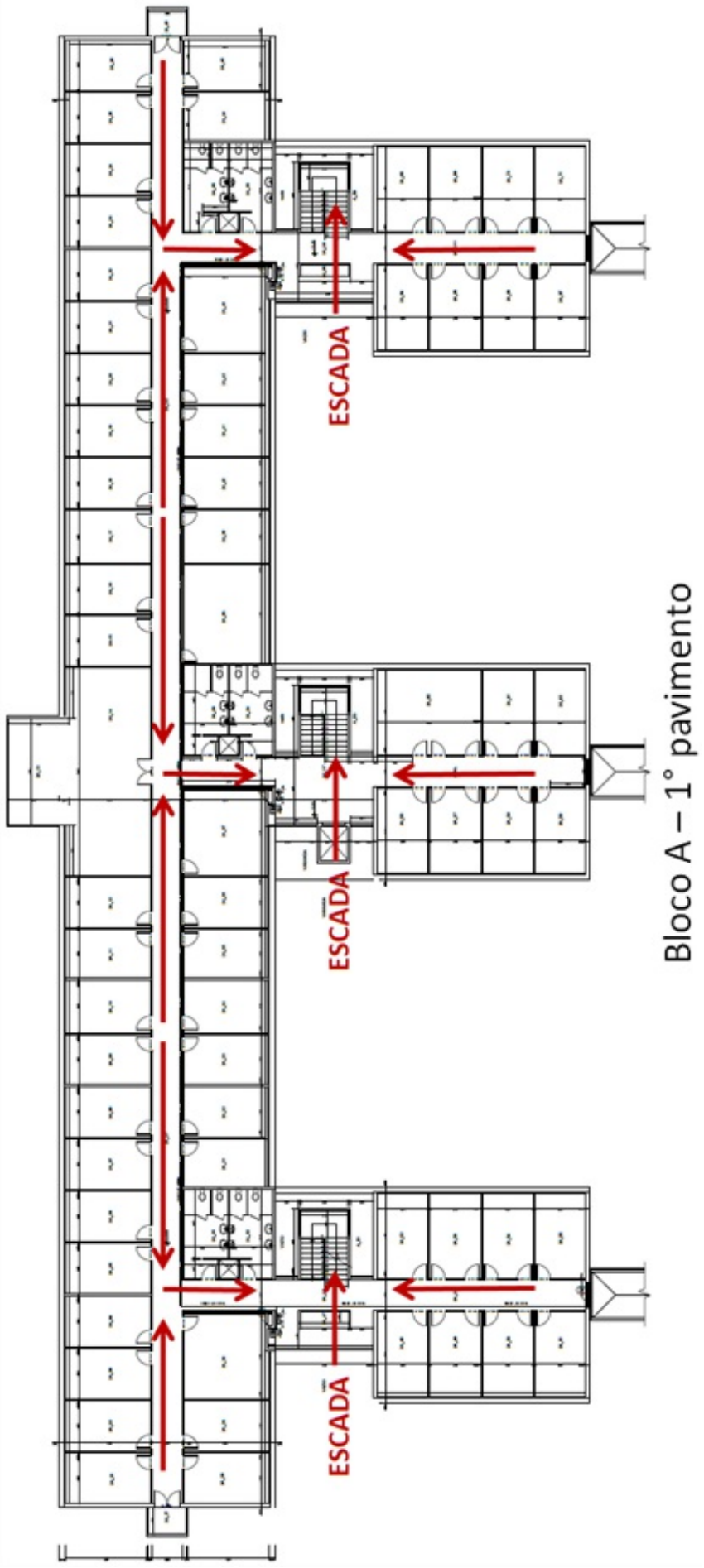
Versão	**Data**	**Descrição**
1.0	17/09/2021	Versão inicial do documento.
2.0	16/06/2023	Revisão geral e adaptação ao novo template.
3.0	12/07/2024	Revisão da formatação e atualização de informações.
4.0	21/08/2025	Atualização conforme a versão da ISO de 2022
4.1	18/11/2025	Ajuste no formato do documento para o SEI

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Vitor de Souza Colimodio	Chefe do SECAM
Verificado por:	Luís Rodrigo de Oliveira Gonçalves	Gestor de Segurança da Informação
Aprovado por:	Barbara Paulo Cordeiro Elustondo	Coordenador Substituto da COGEA

ANEXO A – PLANTAS DO LNCC

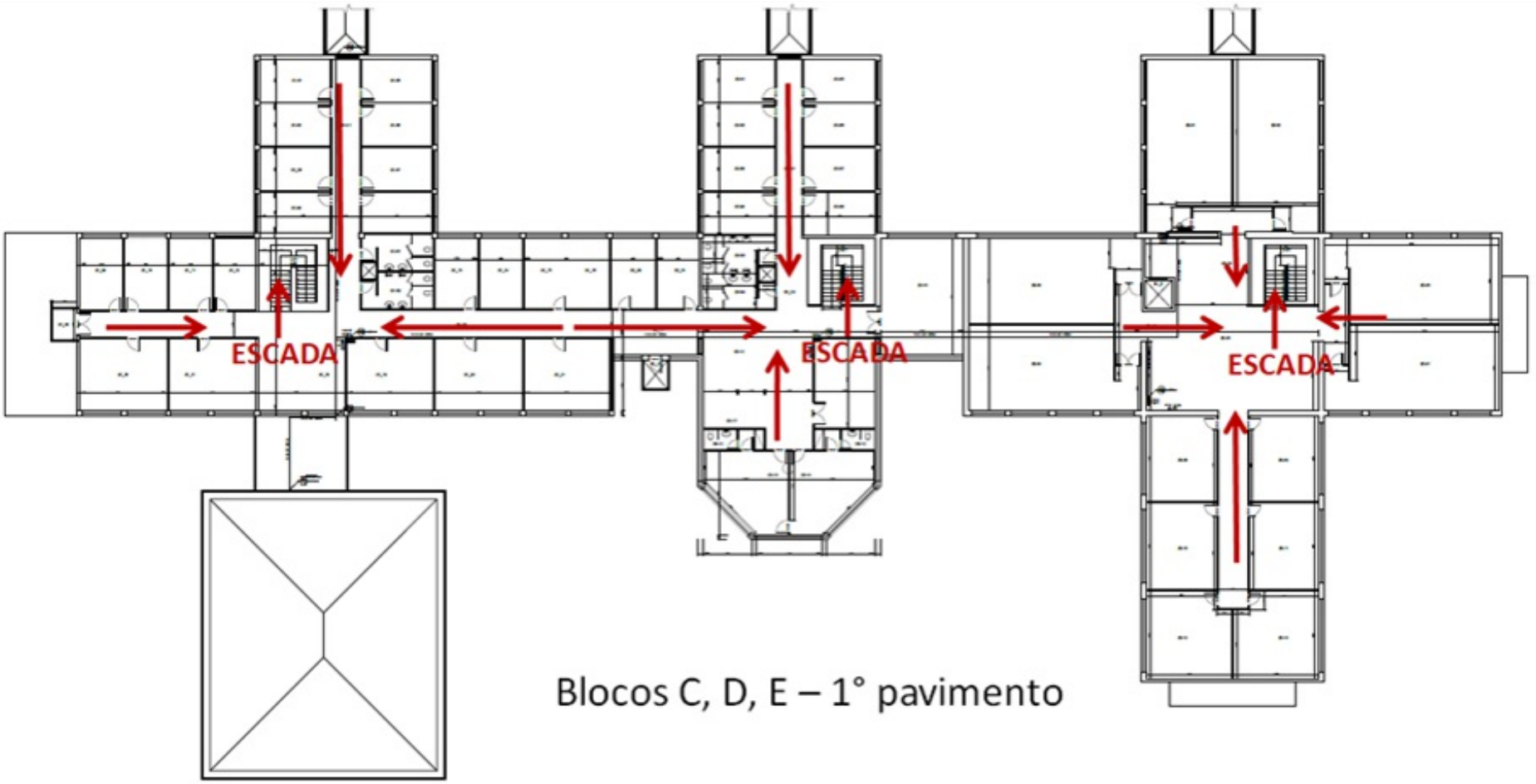


Planta Esquemática Geral

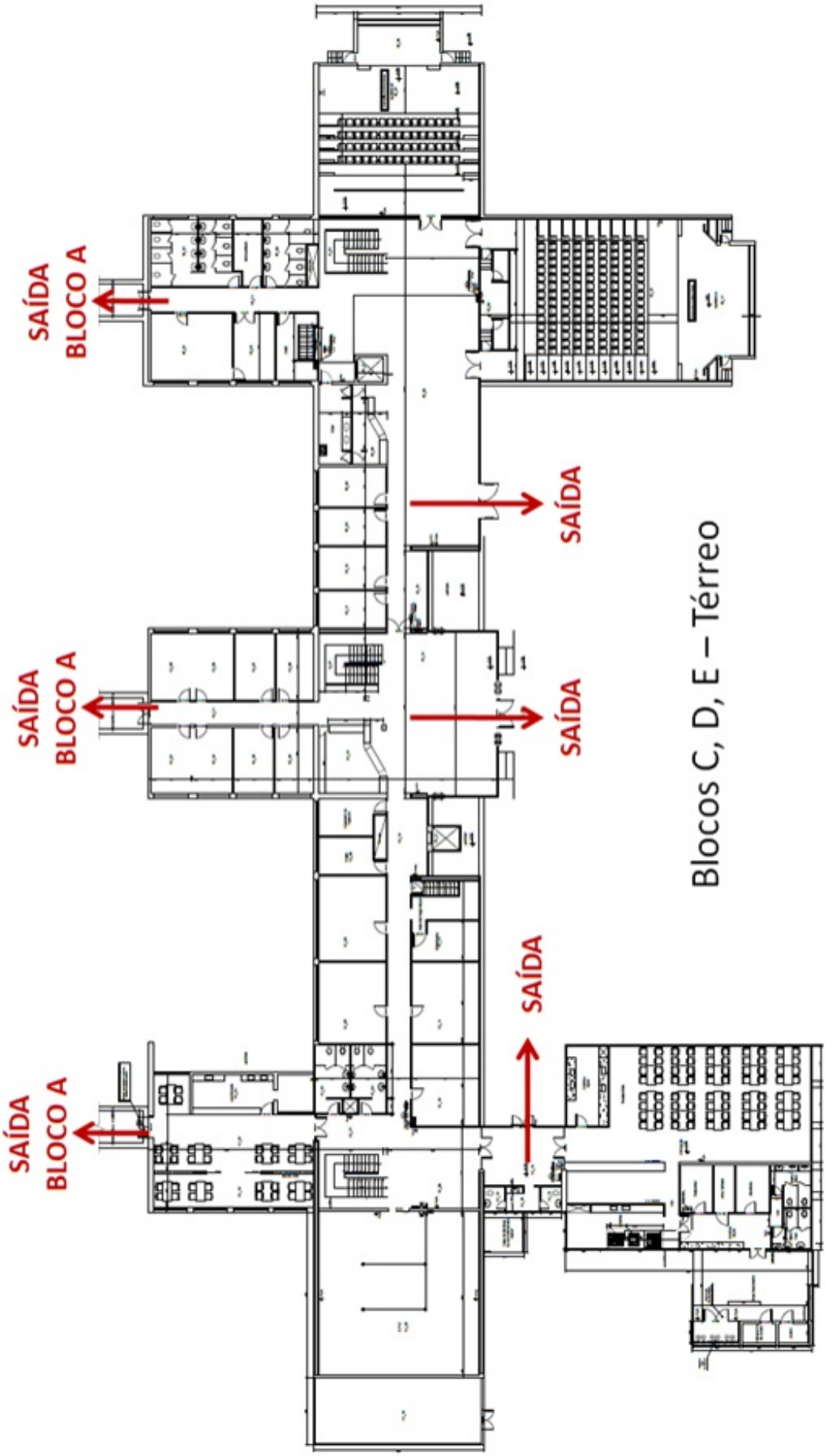


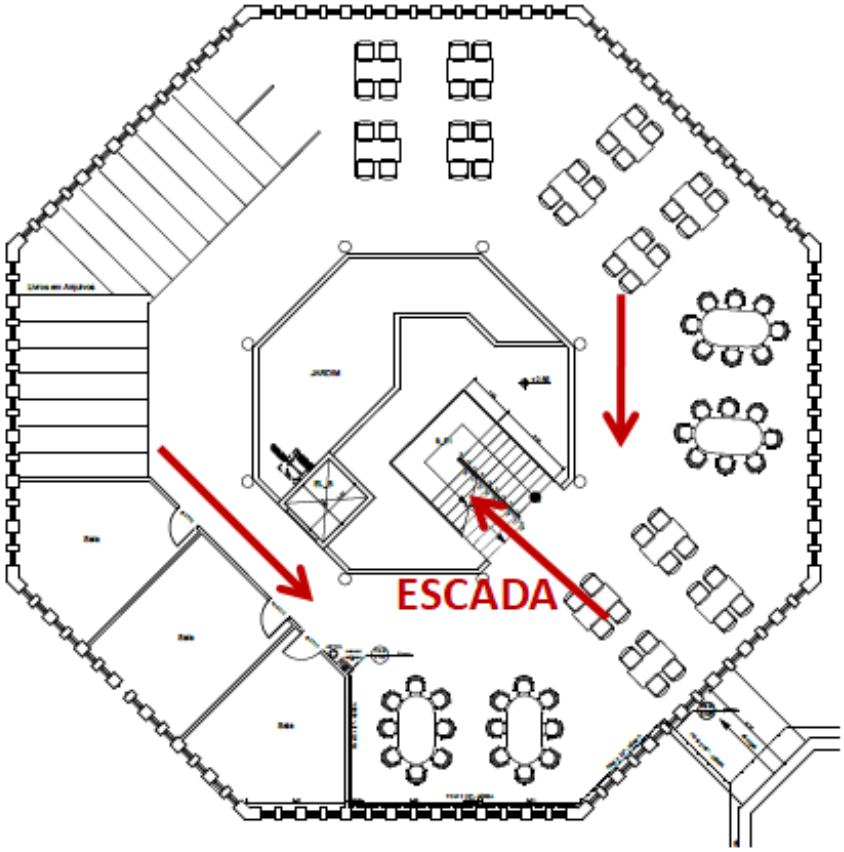
Bloco A – 1° pavimento

Bloco A – Térreo

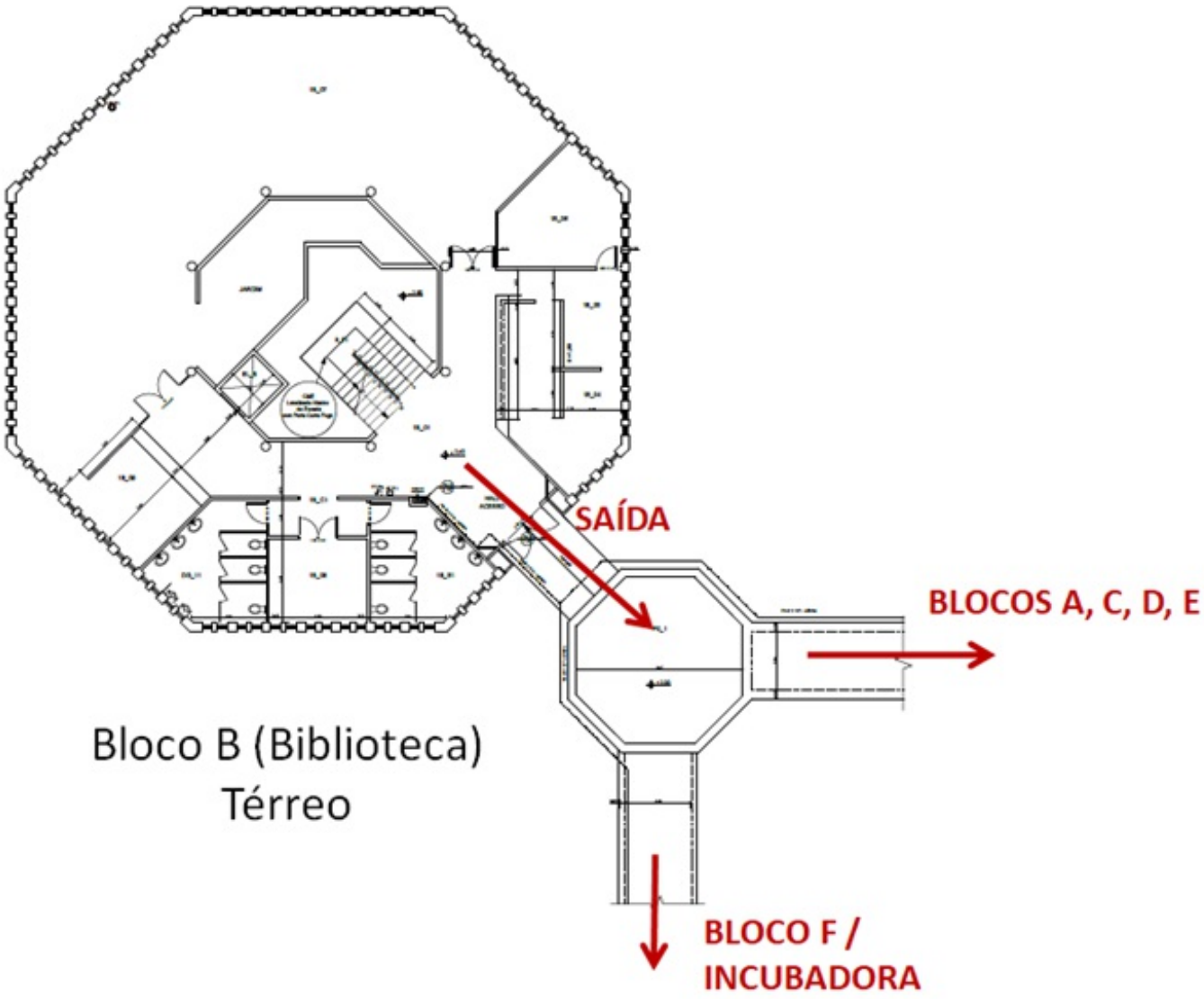


Blocos C, D, E – 1° pavimento

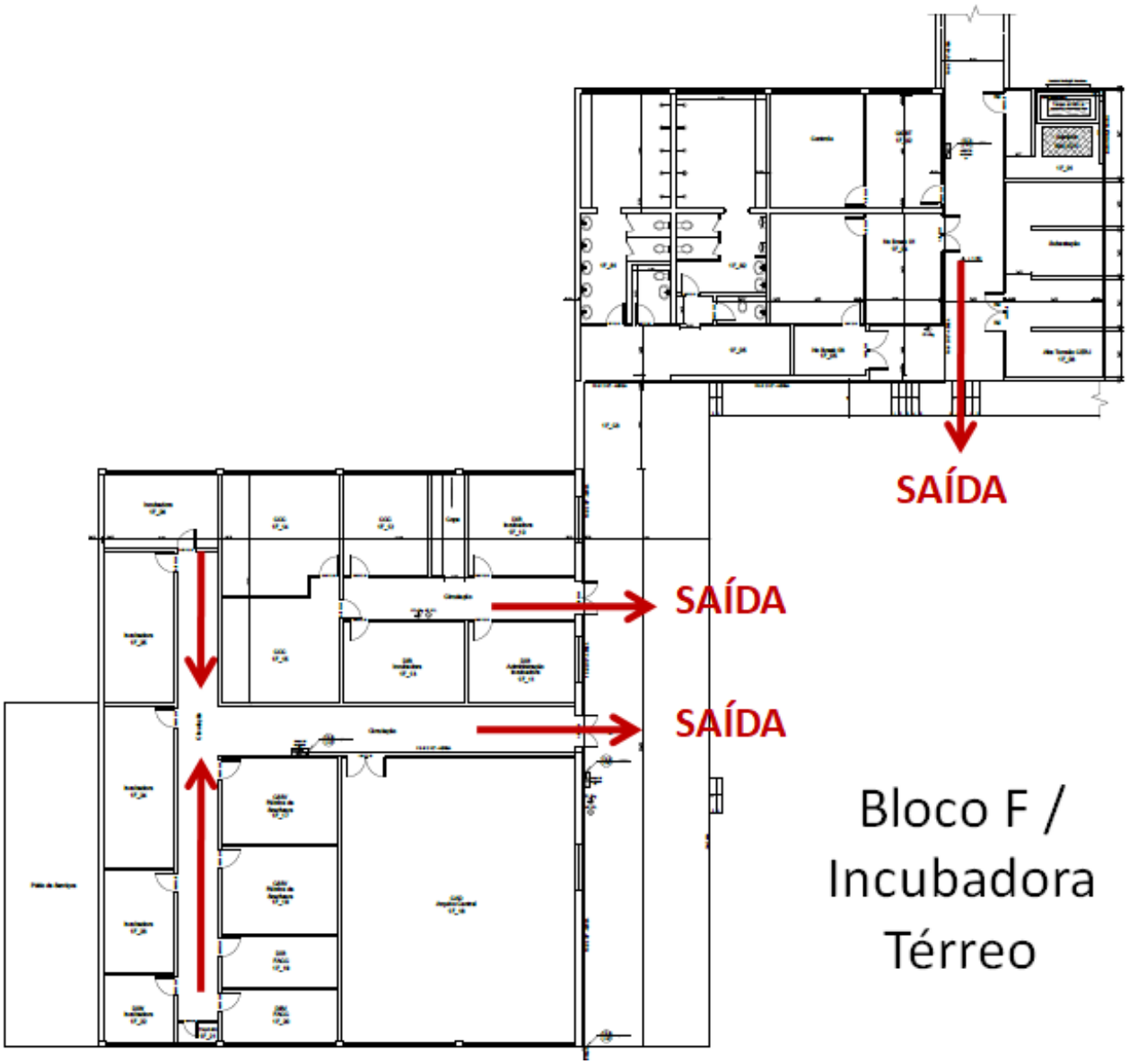

SAÍDA
BLOCO A
SAÍDA
SAÍDA
BLOCO A
SAÍDA
SAÍDA
SAÍDA
BLOCO A
Blocos C, D, E – Térreo



Bloco B (Biblioteca) – 1° pavimento



Bloco B (Biblioteca)
Térreo



Documento assinado eletronicamente por **Luis Rodrigo De Oliveira Gonçalves**, **Gestor de Segurança da Informação**, em 18/11/2025, às 14:06 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Vitor de Souza Colimodio**, **Chefe do Setor de Administração do Campus**, em 18/11/2025, às 15:05 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Bárbara Paulo Cordeiro Elustondo**, **Coordenador de Gestão e Administração substituto**, em 18/11/2025, às 15:55 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **13310984** e o código CRC **2303951F**.