



CRB NACIONAL

Conferência dos Religiosos do Brasil

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) - CONFERÊNCIA DOS RELIGIOSOS DO BRASIL – CRB NACIONAL

CAPÍTULO I – DO PROPÓSITO E OBJETIVOS

Cláusula Primeira – Do Propósito

1.1. A presente Política de Segurança da Informação (PSI) tem por objetivo estabelecer as diretrizes, normas e procedimentos técnicos para garantir a proteção dos ativos de informação da **CRB NACIONAL** contra ameaças internas e externas, intencionais ou acidentais.

1.2. Este instrumento visa assegurar a continuidade das atividades estatutárias da **CRB**, minimizando riscos, prevenindo incidentes cibernéticos e garantindo a preservação da memória, dos dados canônicos e da Vida Religiosa Consagrada no Brasil.

CAPÍTULO II - ESCOPO E ABRANGÊNCIA

Cláusula Segunda – Da Abrangência Obrigatória

2.1. Esta Política aplica-se, sem exceções, a:

- I. **Unidades:** Sede Nacional, Departamentos e, por força do Art. 50 do Estatuto Social, a todas as Secções Regionais e Núcleos;
- II. **Pessoas:** Membros da Diretoria Nacional, Conselho Fiscal, colaboradores (CLT), estagiários, voluntários, prestadores de serviços e terceiros com acesso à rede, sistemas ou dados da CRB;
- III. **Ativos:** Todos os equipamentos (computadores, servidores, dispositivos móveis), sistemas, softwares, redes, bancos de dados e documentos físicos (papel) de propriedade ou sob custódia da CRB.

CAPÍTULO III - PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Cláusula Terceira – Dos Pilares de Segurança e Gestão da Segurança da Informação

3.1. Todas as ações de segurança na **CRB** devem observar os seguintes pilares (CID+A):

- I. **Confidencialidade:** Garantia de que a informação seja acessível somente a pessoas autorizadas;
- II. **Integridade:** Salvaguarda da exatidão e completude da informação e dos métodos de processamento, evitando alterações indevidas;
- III. **Disponibilidade:** Garantia de que os usuários autorizados tenham acesso à informação e aos ativos associados sempre que necessário;
- IV. **Autenticidade:** Garantia de que a informação provém da fonte anunciada e não sofreu alterações não autorizadas.

PARÁGRAFO ÚNICO: As medidas de segurança da informação observarão, no que couber, os princípios previstos na Lei nº 13.709/2018 (LGPD).

Endereço: Edifício Venâncio Ii - Brasília - DF – Brasil

SDS Bloco H - nº 26 - Sala 507

Telefone: (061) 3226 5540

E-mail: crb@crbnacional.org.br

Site: crbnacional.org.br



CRB NACIONAL

Conferência dos Religiosos do Brasil

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

- I. tratamento da informação;
- II. segurança física e do ambiente;
- III. gestão de incidentes em segurança da informação;
- IV. gestão de ativos;
- V. gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;
- VI. controles de acesso;
- VII. gestão de riscos;
- VIII. gestão de continuidade;
- IX. auditoria e conformidade;

CAPÍTULO IV - CLASSIFICAÇÃO DA INFORMAÇÃO

Cláusula Quarta – Níveis de Proteção

4.1. Para fins de aplicação de controles de segurança, as informações da CRB são classificadas em três níveis:

- I. **Pública:** Informações destinadas à divulgação externa (ex: notícias no site, editais públicos, publicações da Editora CRB);
- II. **Interna:** Informações de circulação restrita aos colaboradores e religiosos para a execução de suas tarefas (ex: manuais internos, listas de ramais, rotinas administrativas);
- III. **Confidencial/Sensível:** Informações cujo acesso não autorizado pode causar danos morais, financeiros, canônicos ou jurídicos à CRB ou aos titulares. *Exemplos:* Cadastro de membros, dados de saúde de religiosos, dados sacramentais, folhas de pagamento, senhas, atas de reuniões da Diretoria.

Parágrafo Único: As informações classificadas como Confidencial/Sensível requerem o nível máximo de proteção (criptografia, controle de acesso rigoroso e armazenamento seguro).

CAPÍTULO V - CONTROLE E ENCERRAMENTO DE ACESSO E GESTÃO DE SENHAS

Cláusula Quinta – Do acesso Lógico

5.1. O acesso aos sistemas e rede da **CRB** é individual, pessoal e intransferível.

5.2. Das orientações e disposições acerca das Senhas:

- I. É estritamente proibido compartilhar senhas com colegas, superiores ou subordinados.
- II. As senhas devem possuir complexidade mínima (letras, números e caracteres especiais) e serem trocadas periodicamente.
- III. É vedado anotar senhas em papéis fixados em monitores ("post-its"), sob mesas ou locais visíveis.

Cláusula Sexta – Do Encerramento de Acesso

Endereço: Edifício Venâncio Ii - Brasília - DF – Brasil

SDS Bloco H - nº 26 - Sala 507

Telefone: (061) 3226 5540

E-mail: crb@crbnacional.org.br

Site: crbnacional.org.br



CRB NACIONAL

Conferência dos Religiosos do Brasil

6.1. No momento do desligamento de um colaborador ou término de mandato de um Diretor, todos os seus acessos (e-mail, sistemas, chaves físicas) deverão ser revogados imediatamente pela administração ou departamento competente para fazê-lo, sendo vedada a manutenção de contas de usuário inativas ou genéricas.

CAPÍTULO VI - SEGURANÇA FÍSICA E AMBIENTAL

Cláusula Sétima – Da Política de Mesa Limpa e Tela Bloqueada

7.1. Em consonância com o dever de sigilo previsto no Código de Ética, todos devem observar:

- I. **Mesa Limpa:** Documentos classificados como "Confidenciais" ou contendo Dados Pessoais não devem ser deixados sobre as mesas sem supervisão. Devem ser guardados em gavetas ou armários trancados ao final do expediente ou durante pausas.
- II. **Tela Bloqueada:** Ao afastar-se do computador, mesmo que por breves instantes, o usuário deve bloquear a tela (atalho: Windows + L) para impedir visualização ou uso por terceiros.

Cláusula Oitava – Áreas Restritas

8.1. O acesso físico às salas de servidores, arquivos mortos e áreas restritas da Tesouraria/RH é permitido apenas a pessoal autorizado pela Diretoria.

CAPÍTULO VII – DO USO DE ATIVOS TECNOLÓGICOS E INTERNET

Cláusula Nona – Dos Equipamentos (*Hardware*)

9.1. Os computadores e celulares corporativos são ferramentas de trabalho, sendo vedada a instalação de *softwares* piratas, jogos ou programas não homologados pela TI.

9.2. É proibido o uso de dispositivos de armazenamento pessoal (*pen drives*, HDs externos) não autorizados para copiar dados da **CRB**, visando prevenir vazamento de dados e infecção por vírus.

Cláusula Décima – Do E-mail Corporativo e Internet

10.1. O e-mail corporativo (@crbnacional.org.br ou domínios regionais) deve ser usado exclusivamente para fins profissionais.

10.2. É vedado o envio de correntes, conteúdo ofensivo, pornográfico ou que atente contra a moral cristã e os valores da CRB.

Cláusula Décima Primeira – Do Monitoramento

Endereço: Edifício Venâncio Ii - Brasília - DF – Brasil
SDS Bloco H - nº 26 - Sala 507
Telefone: (061) 3226 5540
E-mail: crb@crbnacional.org.br
Site: crbnacional.org.br



CRB NACIONAL

Conferência dos Religiosos do Brasil

11.1. A **CRB** reserva-se o direito de monitorar e auditar o uso dos recursos tecnológicos (e-mail, internet, logs de acesso e arquivos), para garantir a segurança da informação e a conformidade legal, conforme ciência dada nos Termos de Uso e Contratos de Trabalho.

CAPÍTULO VIII - PROTEÇÃO DE DADOS E PRIVACIDADE (LGPD)

Cláusula Décima Segunda – Integração com a PPSI

12.1. Esta PPSI deve ser interpretada e aplicada em total consonância com a Política Interna de Privacidade e Proteção de Dados (PPSI) da CRB.

12.2. Qualquer extração de relatórios, listas de membros ou bases de dados para envio a terceiros devem ser previamente autorizada pelo Encarregado de Dados (DPO) ou pela Diretoria, garantindo-se a criptografia ou proteção por senha do arquivo.

CAPÍTULO IX - CÓPIAS DE SEGURANÇA (BACKUP)

Cláusula Décima Terceira – Da Rotina de Backups

13.1. A **CRB** manterá rotina de *backups* (cópias de segurança) periódicos de seus servidores e bancos de dados críticos.

13.2. É dever de cada colaborador salvar seus arquivos de trabalho na rede corporativa ou na nuvem oficial da instituição (ex: OneDrive/Sharepoint corporativo). Arquivos salvos apenas na "Área de Trabalho" (Desktop) local do computador não possuem garantia de *backup* e são de risco exclusivo do usuário.

CAPÍTULO X - TRABALHO REMOTO E DISPOSITIVOS MÓVEIS

Cláusula Décima Quarta – Segurança em Home Office e Mobilidade

14.1. Em caso de trabalho remoto ou uso de notebook corporativo fora da sede:

- I. É vedado ao usuário utilizar redes *Wi-Fi* públicas abertas (sem senha) para acessar sistemas da **CRB**, devido ao risco de interceptação de dados;
- II. Em caso de roubo ou furto do equipamento, o fato deve ser comunicado imediatamente à Diretoria e à TI para bloqueio remoto de acessos e alteração de senhas.

CAPÍTULO XI – GESTÃO DE INCIDENTES DE SEGURANÇA

Cláusula Décima Quinta – Dever de Comunicação

Endereço: Edifício Venâncio li - Brasília - DF – Brasil
SDS Bloco H - nº 26 - Sala 507
Telefone: (061) 3226 5540
E-mail: crb@crbnacional.org.br
Site: crbnacional.org.br



CRB NACIONAL

Conferência dos Religiosos do Brasil

15.1. Todo colaborador, religioso ou terceiro que identificar uma fragilidade ou incidente de segurança (ex: suspeita de vírus, e-mail de *phishing*, tentativa de invasão, vazamento de papel com dados) deve reportar o fato imediatamente ao canal de suporte de TI ou ao Encarregado de Dados (DPO).

15.2. É vedado ao usuário investigar ou tentar resolver incidentes de segurança complexos por conta própria, a fim de preservar as evidências digitais.

15.3. Todos os contratos de prestação de serviços firmados pela **CRB**, conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como de suas normas decorrentes.

CAPÍTULO XII – DAS PENALIDADES

Cláusula Décima Sexta – Da Violação das Normas

16.1. A violação das normas desta Política é considerada infração grave, colocando em risco a operação, a segurança jurídica e a reputação da **CRB**.

16.2. O infrator estará sujeito às sanções disciplinares previstas no **CAPÍTULO 10 (Medidas Disciplinares) do Código de Ética e Conduta**, que incluem:

- a. Advertência verbal ou escrita;
- b. Suspensão;
- c. Demissão por justa causa ou destituição de função, sem prejuízo das responsabilidades civis e penais (Lei de Crimes Cibernéticos e LGPD).

CAPÍTULO XIII – DAS DISPOSIÇÕES FINAIS

Cláusula Décima Sétima – Vigência, Casos Omissos e Foro

17.1. Esta Política entra em vigor na data de sua aprovação pela Diretoria Nacional.

17.2. Os casos omissos serão tratados pela Diretoria Nacional com apoio da Assessoria de TI e Jurídica.

17.3. A presente política deverá ser revisada anualmente ou quando houver mudanças significativas na infraestrutura tecnológica.

17.4. Fica eleito o Foro de Brasília/DF (conforme **Art. 4º do Estatuto Social**) para dirimir quaisquer questões oriundas desta Política.

Endereço: Edifício Venâncio li - Brasília - DF – Brasil
SDS Bloco H - nº 26 - Sala 507
Telefone: (061) 3226 5540
E-mail: crb@crbnacional.org.br
Site: crbnacional.org.br



CRB NACIONAL

Conferência dos Religiosos do Brasil

Brasília/DF, 01 de janeiro de 2026.

Ignia Distero Rocha, FCI, M

Presidente da Conferência dos Religiosos do Brasil



Endereço: Edifício Venâncio Ii - Brasília - DF – Brasil
SDS Bloco H - nº 26 - Sala 507
Telefone: (061) 3226 5540
E-mail: crb@crbnacional.org.br
Site: crbnacional.org.br