Política de Segurança da Informação

Julho de 2026

Este documento contou com a contribuição do ICNR (consultor externo)

Sumário

1 | OBJETIVO

Tendo em vista o compromisso do **INR**, que consistem nas empresas **INR Contábil Ltda, Herance Sociedade de Advogados** e **Boletins Informativos Ltda.** Publicações ("INR"), com a proteção das informações que estão sob sua guarda, é publicada esta Política de Segurança da Informação.

Esta política estabelece as diretrizes e critérios sobre melhores práticas para garantir a confiabilidade das informações, através da preservação de sua confidencialidade, integridade e disponibilidade.

2 | LEGISLAÇÃO APLICÁVEL

- Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);
- Lei de Acesso à Informação (Lei nº 12.527/2011);
- Marco Civil da Internet (Lei nº 12.965 de 23/04/2014); e
- Norma de melhores práticas ISO/ISC 27001/2 e 27701.

3 | ABRANGÊNCIA

Esta política se aplica a todos aqueles que, ainda que transitoriamente, tenham acesso às informações e processos de negócios do INR sendo fundamental a participação das partes interessadas em sua aplicação e atualização.

De maneira especial, esta política deve orientar a atuação de gestores, colaboradores e fornecedores do INR.

4 | DEFINIÇÕES

Para fins da presente política, consideram-se:

- **Alta Direção**: delimita as pessoas que exerçam função gerencial, com poder de decisão sobre as atividades do INR;
- **Ameaça**: elemento externo capaz de explorar vulnerabilidades existentes que pode ocasionar prejuízo em um sistema ou a uma organização;
- **Análise de Risco**: identificação e avaliação dos riscos (vulnerabilidades e impactos) a que os ativos da informação estão sujeitos;
- **Backup**: processo de extração de cópia dos dados do ambiente operacional do INR, que será utilizada numa situação de incidentes ou desastres que venham a ocorrer;

- **Classificação da Informação**: processo que compreende a identificação e definição de níveis e critérios de proteção para as informações, de forma a garantir sua confidencialidade, integridade e disponibilidade;
- **Confiabilidade da Informação**: recurso relativo à consistência no comportamento e nos resultados desejados;
- **Confidencialidade da Informação**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Controle de Acesso Físico**: controles e ações implementados no INR com a finalidade da proteção das informações;
- **Disponibilidade da Informação**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes tempestivamente (no momento da solicitação);
- **Gestão de Risco**: atividades coordenadas para dirigir e controlar uma organização em relação ao risco, aplicabilidade de suas políticas de segurança bem como monitoramento e revisão dos riscos;
- **Gestão de Mudanças**: processo utilizado para controlar as mudanças realizadas no INR;
- **Governança da Segurança da Informação**: conjunto de princípios e processos os quais o INR adota e utiliza-se para dirigir e monitorar as atividades relacionadas com a segurança da informação;
- **Impacto**: trata das consequências esperadas caso as informações protegidas sejam expostas de forma não autorizada;
- **Informação**: conteúdo de valor para a organização ou o profissional que deverá ser protegida e mantida;
- **Integridade da Informação**: salvaguarda da exatidão e completeza da informação;
- **Inventário de Ativos de Informação**: documentos físicos e digitais tratados no INR;
- **Nível de Risco**: importância de um risco ou a combinação de consequências e probabilidades que o risco ocorra. Os critérios de risco são obtidos de normas, leis, políticas e outros requisitos;
- **Plano de Continuidade do Negócio**: estratégias e planos de ação para garantir que serviços essenciais sejam identificados, bem como sua preservação após a ocorrência de um desastre, até o retorno da situação normal de funcionamento da instituição.
- **Probabilidade**: oportunidade de uma vulnerabilidade ser explorada por uma ameaça;
- **Risco**: estabelece a relação entre probabilidade e impacto, ajudando a determinar onde concentrar investimentos em segurança da informação;
- **Segurança da Informação**: medidas praticadas para garantir a preservação dos dados em face de ameaças que podem afetar sua disponibilidade, integridade, confidencialidade ou confiabilidade;
- **Segurança**: medidas de proteção contra perigos, ameaças e incertezas; e
- **Vulnerabilidade**: fragilidade de um ativo ou de um controle que pode ser explorado por uma ou mais ameaças.

5 | SEGURANÇA DE INFORMAÇÕES

A Segurança de Informações deve ser de uso contínuo e voltado para a proteção dos ativos de informação, tendo como requisitos básicos:

- Preservação da **Integridade** das informações - Pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;
- Maior **disponibilidade** das informações - Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática; e
- **Confidencialidade** dos dados - Garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal acesso.

6 | ORGANIZAÇÃO DA SEGURANÇA DE INFORMAÇÕES

A organização da segurança de informações tem por finalidade orientar os colaboradores do INR quanto à implantação da estrutura operacional e administrativa voltada à proteção das informações.

6.1 | Diretrizes para Organização da Segurança de Informações

O Responsável pela Segurança da Informação, com o aval da Alta Direção, deve assegurar que líderes, coordenadores e demais colaboradores do INR estejam devidamente capacitados para orientar terceiros e clientes em temas relacionados à segurança da informação.

Todos os documentos vinculados à segurança da informação devem ser armazenados em repositório com permissão de leitura acessível a todos os colaboradores do INR.

Líderes e demais colaboradores devem participar, no mínimo uma vez por ano, de treinamentos voltados à segurança da informação.
A manutenção da documentação relativa à segurança da informação deve seguir um cronograma que assegure sua atualização anual; ou sempre que ocorrerem mudanças significativas no INR, ou no mercado.

6.2 | Papeis e Responsabilidades

A adequada gestão da segurança da informação no INR depende da definição clara e formal dos papéis e responsabilidades dos diversos envolvidos nos processos institucionais. Esta estrutura organizacional garante a efetividade das medidas de proteção, bem como a conformidade com as diretrizes estabelecidas nesta Política de Segurança da Informação.

Nesse contexto, são definidos os seguintes agentes responsáveis pela segurança da informação:

6.2.1 | Comitê

O Comitê da LGPD que abarca também as questões da segurança da informação é integrado pela Alta Direção do INR, e tem como atribuições:

- Liderar e garantir que todos os colaboradores conheçam e utilizem a Política de Segurança;
- Definir e manter estratégias relacionadas com segurança de informações;
- Prover recursos e acompanhar a utilização da segurança de informações no INR;
- Dar todo suporte necessário para a área de segurança de informações; e
- Aplicar medidas corretivas, quando necessário.

6.2.2 | Responsável pela Segurança de Informações

O responsável pela segurança de informações tem como atribuições:

- Definir, documentar e manter política, diretrizes, normas e procedimentos de segurança;
- Desenvolver estudos, propor orçamentos e alternativas para atender a segurança de informações;
- Manter inventário de todos os ativos de informação críticos e fazer as manutenções;
- Realizar avaliação de riscos de segurança de informações (anual);
- Assegurar que todas as ações corretivas são realizadas e se eliminaram as não conformidades;
- Reportar os resultados de medições e propor melhorias de segurança e ações corretivas;
- Preparar equipamentos de comunicação para serem utilizados em caso de emergência / desastre;

- Coordenar os exercícios e testes de planos;
- Realizar revisão pós incidente dos planos de recuperação;
- Propor métodos de autenticação, política de senhas, métodos de encriptação etc.;
- Propor regras para trabalho remoto seguro;
- Definir funcionalidades de segurança requeridas para serviços de Internet;
- Definir princípios para o desenvolvimento seguro de sistemas de informação;
- Revisar logs de atividades de usuários de forma a reconhecer comportamentos suspeitos;
- Desenvolver e realizar treinamentos de segurança de informações;
- Receber de líderes requisições de concessão de acessos e criação de usuários;
- Fazer as manutenções e encerramento de acessos e usuários;
- Coordenar o trabalho de avaliação e validação periódica de acessos e utilização de usuários; e
- Dar suporte técnico e direcionamento no que se refere a proteção lógica de ativos de informação.

6.2.3 | Líder da área

Os líderes de cada área são responsáveis por exercitar o papel de proprietário para os ativos que estão sob sua responsabilidade, executando a classificação desses ativos e os protegendo de acordo com as políticas de segurança de informações.

6.3 | Repositório de Segurança de Informações

O conjunto de documentos de políticas, diretrizes, normas e procedimentos de segurança de informações devem ser organizados e armazenados num arquivo especialmente disponibilizado para esse fim, que chamamos de Repositório de Segurança de Informações.

7 | POLÍTICA DE SEGURANÇA DE INFORMAÇÕES

Esta Política de Segurança de Informações é uma declaração formal e geral da Alta Direção do INR, que define o papel da segurança de informações dentro da organização. Ela provê orientação e direcionamentos para atender seus requisitos de negócios, leis, norma de melhores práticas de segurança de informações (ISO 27001), regulamentações relevantes para seus níveis estratégico, tático e operacional.

7.1 | Gestão de Segurança

A segurança da informação deve ser compartilhada entre todos os diretores, líderes e colaboradores do INR, considerando que:

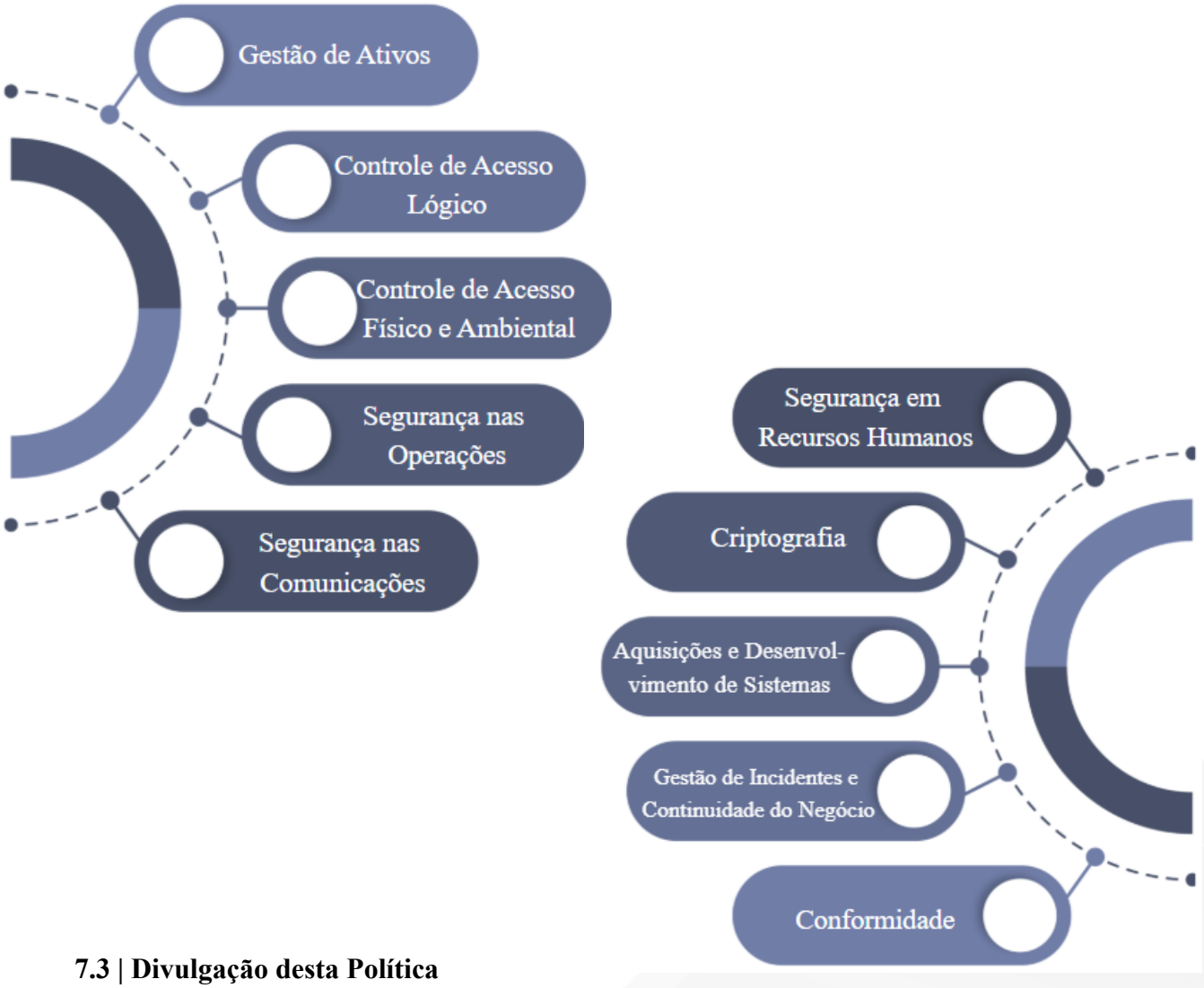
- Compete ao Comitê da LGPD a definição de padrões e direcionamentos, para garantir que a segurança das informações estará devidamente tratada no INR;
- **Todos os colaboradores e terceiros devem assinar (terceiros, apenas o primeiro)**:
  - **TERMO DE COMPROMISSO** – Anexo I deste documento.
  - **TERMO DE COMPROMISSO DE USO DE HARDWARE E SOFTWARE** – Documento INR; e
  - **TERMO DE TRATAMENTO DE DADOS** – Documento INR.
- Caberá às demais áreas e seus colaboradores aderir a estes padrões e direcionamentos, garantindo a efetiva segurança das informações.

7.2 | Estrutura desta Política de Segurança de Informações

A ISO/ISC 27001/2 e 27701 são as normas de melhores práticas que trata da Segurança de Informações e Privacidade e está dividida em módulos que compõem a Política de Segurança de Informações utilizadas nas organizações em todo mundo.

Neste documento de Política de Segurança são tratados desses módulos que deverão ser utilizados como direcionamento para atender aos requisitos de segurança de informações.

Os módulos apresentados a seguir são os seguintes:



7.3 | Divulgação desta Política

A alta direção, líderes e colaboradores do INR possuem a responsabilidade pela divulgação ampla desta Política de Segurança de Informações para todos os usuários internos e externos, pois ela deve ser de conhecimento de todos que, de algum modo, interagem com o INR.

7.4 | Penalidades

As falhas e utilização indevida dos direcionamentos de segurança da informação definidos nesta Política de Segurança, pelos colaboradores do INR, exigirá dos diretores e líderes a aplicação de medidas corretivas cabíveis, chegando inclusive ao desligamento do colaborador, caso haja uma situação grave.

Dessa forma, fica ainda mais evidente a importância da conscientização dos colaboradores quanto à Política de Segurança, garantindo que ela seja de conhecimento de todos no INR. Não será admissível que as pessoas aleguem ignorância quanto às regras nela estabelecidas a fim de livrarem-se da culpa sobre violações cometidas.

É importante salientar que quando detectada uma violação, é preciso averiguar as causas, consequências e circunstâncias em que ocorreu. Pode ter sido derivada de um simples acidente, erro ou mesmo desconhecimento da Política de Segurança, negligência, ação deliberada e fraudulenta.

Essa averiguação possibilita que vulnerabilidades até então desconhecidas pelo time da área de segurança de informações passem a ser consideradas, exigindo, se for o caso, alterações na Política de Segurança.

8 | GESTÃO DE ATIVOS

A Gestão de Ativos tem como objetivo definir critérios e direcionamentos para identificar os ativos de informação, definir as responsabilidades apropriadas para sua proteção e assegurar que as informações recebam o nível adequado de proteção, de acordo com a sua importância para o INR.

8.1 | Nomenclatura

Proprietário é a pessoa responsável pelo ativo de informação, no que se refere **em sua criação, manutenção, autorização e eliminação de acessos**. O proprietário atua como "dono" do ativo de informação e é responsável pela sua classificação, que orientará a forma de proteção do ativo.

O proprietário normalmente é um líder da área onde foi criado e mantido o ativo de informação Ex. cadastro de clientes, manual de preços, mapas e desenhos etc.

Responsável pela guarda da informação é a pessoa ou área incumbida de armazenar, manter e proteger os ativos de informação, em conformidade com as diretrizes estabelecidas pelo Proprietário do ativo. Por exemplo, a área de Tecnologia da Informação (TI) atua como responsável pela guarda de informações pertencentes a diversas áreas do INR, garantindo sua proteção conforme as orientações dos respectivos proprietários. Essa função também pode ser exercida por empresas terceirizadas, como escritórios de contabilidade, assessorias jurídicas, empresas de engenharia, entre outras, desde que formalmente designadas.

8.2 | Diretrizes de Gestão de Ativos

Os líderes do INR são responsáveis por garantir que todos os ativos de informação (documentos, arquivos, contratos, bancos de dados, computadores, armários etc.) sob sua responsabilidade, sejam classificados de acordo com sua importância.

Na definição da classificação para os ativos de informação, os proprietários devem evitar que sejam supervalorizados os níveis de classificação, pois pode tornar a operacionalidade mais complexa do que deveria. A subclassificação, por outro lado, pode trazer uso indevido de informações. Dessa forma, é mandatório que as classificações sejam feitas de forma cuidadosa e em caso de dúvidas o proprietário deve buscar ajuda de outros líderes ou da área de segurança de informações.

A área de TI somente concederá acessos à ativos de informação com a autorização e definições dos proprietários desses ativos.

Após a utilização de um ativo de informação e esse acesso não sendo mais necessário, o colaborador ou seu líder imediato devem pedir à área de TI para cancelar as autorizações de acesso.

Nenhum colaborador pode conceder acessos a ativos de informação sem a devida autorização do proprietário desses ativos de informação.

Os líderes devem fazer periodicamente uma avaliação dos acessos concedidos e usuários, que estão sob sua responsabilidade (colaborador e prestadores de serviços). Após essa análise devem ser feitos os acertos definidos como necessários para atender a segurança de informações.

A área de TI deverá trimestralmente revisar junto aos líderes se existe uma validação dos acessos e usuários que estão sob sua responsabilidade. A seguir o líder deve comandar as atualizações de utilização dos ativos de informação.

8.3 | Classificação da Informação

Os líderes e demais colaboradores devem assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para o INR. As informações devem ser classificadas em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. A tabela a seguir apresenta fatores que devem ser considerados no estabelecimento da classificação dos ativos de informação do INR.

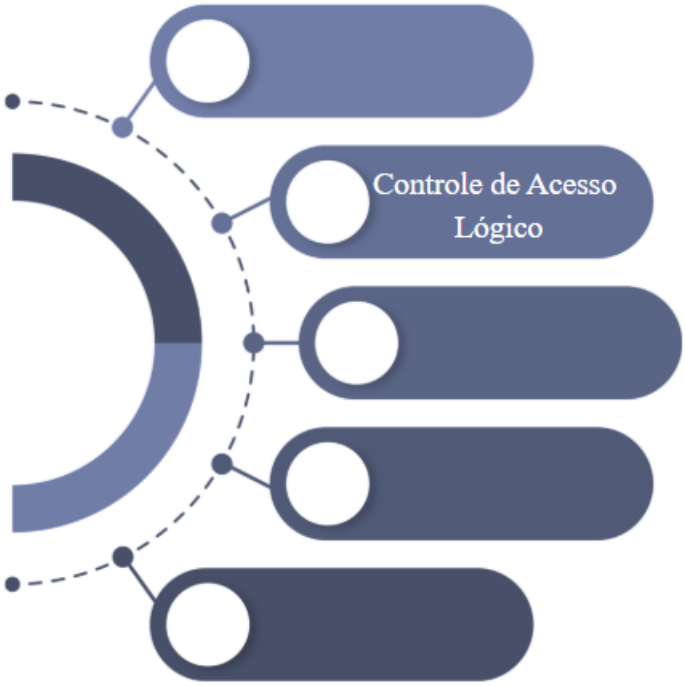
Rótulos	Finalidade do Uso
Uso Público	São ativos de informação de conhecimento geral dentro e fora do INR. ex. prospectos, apresentações, demais material de marketing etc.
Uso Interno	São utilizados como ativos de informação de uso geral somente dentro do INR. ex. tabelas, gráficos, relatórios em geral etc.
Uso Restrito	São utilizados como ativos de informação de uso geral apenas para uma determinada área. ex. tabelas, gráficos, relatórios em geral etc.
Uso Confidencial	Ativos de informação importantes que só algumas pessoas podem conhecer. ex. resultado de testes de projetos, contratos de clientes, planejamentos operacionais etc.

8.4 | Procedimento da Classificação

Uma vez classificado o ativo, é importante que a informação seja rotulada para que o seu nível de proteção seja facilmente identificado. No caso de informações no formato eletrônico, onde não é possível utilizar rótulos físicos, o nível de classificação deve, de algum modo, ser apresentado no próprio documento ou na nomenclatura do documento.

A classificação poderá ser operacionalizada por meio de ferramentas tecnológicas (ex.: Microsoft 365), com rotulagem manual ou automática dos documentos.

9 | CONTROLE DE ACESSO LÓGICO



O objetivo do Controle de Acesso Lógico é **disponibilizar regras e meios para proteger os ativos de informações do INR**, permitindo assim garantir sua disponibilidade, confidencialidade e integridade, cumprindo requisitos legais, requisitos das agências reguladoras e as melhores práticas definidas pela norma ISO 27001/2 que trata da segurança de informações.

9.1 | Diretrizes do Controle de Acesso Lógico

Os acessos deverão ser concedidos de **forma controlada e em bases de necessidades de negócios (*need to know*) e necessidade de uso**, sempre prevalecendo o atendimento da confidencialidade, autenticidade e disponibilidade.

Todos os acessos devem ser concedidos com **aprovação do proprietário dos ativos de informações**, sejam para funcionários regulares ou prestadores de serviços.

Os usuários são responsáveis pela proteção das informações manuseadas, na execução dos serviços no dia a dia e em hipótese alguma podem disponibilizá-las a outros usuários não autorizados.

Líderes e responsáveis pela guarda de dados devem orientar os usuários a seguir as práticas de segurança de informação, no momento da liberação dos acessos concedidos.

O líder responsável pelo ativo de informação (proprietário) deve fazer sua classificação, de acordo com sua importância para os negócios do INR. Essa classificação deve ser passada para a área de TI que viabilizará a proteção desses ativos de informação.

É mandatório que o uso de programas utilitários, que podem ser capazes de sobrepor os controles dos sistemas e aplicações, sejam restritos e estritamente controlados.

Os acessos privilegiados (diretórios, sistemas, arquivos etc.) devem ser rigorosamente controlados e quando concedidos, deverão ser por períodos curtos e com avaliações periódicas (trimestrais).

9.2 | Responsabilidades

O líder do colaborador deve interagir com a área de TI, para adequar a solicitação de acesso e justificar a necessidade de concessão, para seu colaborador. O proprietário do ativo de informação é responsável por analisar a requisição de acesso e aprovar a concessão, desde que atendam as regras de "need to know" para atender as necessidades de negócio.

Cada colaborador do INR no ato de sua admissão recebe um usuário para utilização em suas atividades do dia a dia em sua área de trabalho. O acesso será concedido mediante preparação prévia do equipamento pela área de TI, com credenciais já configuradas conforme o perfil do colaborador.

Os usuários devem obedecer rigorosamente às regras e direcionamentos de segurança de informações do INR. O líder do colaborador será responsável por aprovar a concessão do usuário, pela utilização do mesmo durante a estadia deste na empresa e pela revogação no seu desligamento.

O uso compartilhado de ID de usuário somente será permitido onde eles são necessários por razões operacionais ou de negócios. **Convém que seja aprovado e documentado**.

É mandatório que haja imediata remoção ou desabilitação do usuário que tenha deixado o INR voluntariamente ou por desligamento.

É mandatório que os líderes analisem periodicamente os usuários e acessos que não mais estão sendo utilizados e façam sua remoção e desabilitação.

Toda e qualquer programa/sistema/software/aplicativo que exija MFA (Multifator de Autenticação), o segundo fator de autenticação será gerenciado pela área de TI do INR, não sendo permitido uso em dispositivos pessoais dos usuários, como medida de controle e segurança.

9.3 | Utilização de Programas e Ferramentas com Privilégios

O uso de programas e ferramentas que possuam capacidade de sobrepor ou contornar os controles estabelecidos nos sistemas e aplicações deve ser rigorosamente controlado. A concessão e o uso de acessos privilegiados devem ser restritos e gerenciados pelos respectivos responsáveis, conforme os procedimentos definidos para a concessão de permissões.

9.4 | Diretrizes de Utilização de Correio Eletrônico

O correio eletrônico é uma ferramenta extremamente importante para as operações do dia a dia, mas deve ser protegida contra usos indevidos por terceiros.

A seguir são apresentadas algumas orientações e diretrizes para utilização de correio eletrônico:

- Os sistemas de e-mail fornecidos pelo INR só podem ser utilizados para fins de trabalho ou propósitos com assuntos gerais relacionados ao trabalho;
- O INR reserva-se o direito de arquivar e-mails eletronicamente, verificá-los para detectar vírus, apresentá-los a auditores internos e externos, usá-los como evidência em conexão com processos judiciais ou regulatórios e usá-los outros propósitos comerciais;
- Os e-mails estão sujeitos a obrigações legais de retenção, que devem ser seguidas no INR;
- Os usuários devem tomar providências em caso de ausência (por exemplo, doença, férias);
- O INR tem direito a acessar os e-mails do usuário, no caso de necessidades de negócios ou qualquer outra;
- Todo usuário deve estar ciente de que os e-mails privados podem ser lidos, mesmo que não estejam relacionados ao trabalho;
- **Os e-mails encaminhados para endereços de e-mail não INR são explicitamente proibidos**; e
- Não é permitido o uso de contas de e-mail privadas para fins de trabalho.

9.5 | Acessos à Internet e Intranet

A internet é uma ferramenta extremamente importante para o INR e deve ser utilizada obedecendo critérios para administração e utilização dos acessos aos serviços de **Internet** e **Intranet**.

Internet

O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo INR, observando-se sempre a conduta compatível com a moralidade administrativa. Os seguintes itens são VEDADOS:

- Acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: pornografia, pedofilia, preconceitos, vandalismo, entre outros;
- Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede do INR;
- Uso de Messenger não homologado ou autorizado;
- Uso recreativo da internet em horário de expediente;
- Acesso a salas de bate-papo (chats), exceto aqueles definidos como ferramenta de trabalho homologada pelo INR;
- Acesso a rádio e TV em tempo real, exceto os canais corporativos;
- Acesso a jogos de qualquer espécie;
- Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;
- Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, micro blogs, ou ferramentas semelhantes;
- Envio a destino externo de qualquer software licenciado do INR ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;
- Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do INR;
- Utilização de softwares de compartilhamento de conteúdo na modalidade peer-to-peer (P2P);
- Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação do INR, na forma definida pela área de TI.

Intranet

O acesso à Intranet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo INR, observando-se sempre a conduta compatível com a moralidade administrativa.

O acesso aos serviços de Intranet deve ser realizado mediante autenticação da conta do usuário, sendo que todos os acessos realizados serão auditados, constituindo um histórico de acessos, podendo ser consultado ou publicado a critério da instituição.

9.6 | Senhas

Todo acesso aos recursos de TI deve ser protegido por uma senha segura na medida tecnicamente possível. Os colaboradores devem obedecer a política de senhas. Todos os usuários devem:

- Manter a confidencialidade das senhas;
- Não compartilhar senhas;
- Evitar o registro de senhas em papel;
- Selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que os obriguem a escrevê-las em um pedaço de papel (recomenda-se tamanho igual ou maior que oito caracteres);
- Alterar a senha sempre que existir indicação de possível comprometimento do sistema ou da própria;
- Alterar a senha em intervalos regulares ou com base no número de acessos (senhas para usuários privilegiados devem ser alteradas com maior frequência que senhas normais);
- Evitar reutilizar as mesmas senhas;
- Alterar senhas temporárias no primeiro acesso ao sistema;
- Não incluir senhas em processos automáticos de acesso ao sistema (ex. armazenadas em macros).
- Evitar utilizar a mesma senha para vários sistemas;
- Os usuários devem evitar senhas compostas de elementos facilmente identificáveis por possíveis invasores, como por exemplo:
    - Nome do usuário, mesmo que os caracteres estejam embaralhados;
    - Nome de membros de sua família ou de amigos íntimos;
    - Nomes de pessoas ou lugares em geral;
    - Nome do sistema operacional ou da máquina que está sendo utilizada;

- Nomes próprios, datas, nº telefone, de cartão de crédito, de carteira de identidade e outros;
- Placas ou marcas de carro; letras ou nºs repetidos; letras seguidas do teclado do computador.

- Adquira o hábito de trocar sua senha com frequência. Trocá-la a cada 90 dias é uma boa prática; e
- Não compartilhe suas senhas, no caso de necessidade a área de TI deve criar uma senha específica e documentar esse tipo de utilização.

10 | SEGURANÇA FÍSICA E AMBIENTAL

O objetivo da Segurança Física e Ambiental é definir e disponibilizar conjunto de direcionamentos, políticas, diretrizes, normas e procedimentos para atender a segurança de informações, no que que se refere ao perímetro de segurança, vizinhança, infraestrutura física e ferramentas de apoio de controle a acessos.

10.1 | Diretrizes de Segurança Física e Ambiental

O perímetro de segurança deve ser delimitado, identificado e protegido de acessos não autorizados.

O acesso físico nas instalações do INR deve ser controlado e orientado, de maneira a disciplinar a movimentação e circulação de pessoas, materiais, equipamentos documentados e veículos.

Acessos aos componentes de infraestrutura das instalações do INR devem ser controlados e restritos.

O acesso de pessoas ao INR deve ser condicionado ao cadastro prévio e a identificação pela segurança.

A presença de visitantes deve ser acompanhada de profissional do INR.

O colaborador deverá responder por todo e qualquer acesso físico aos ativos do INR sob sua responsabilidade.

10.2 | Áreas Controladas

As áreas controladas consistem no nível 1 (ex. áreas internas do INR) e nível 2 (ex. TI, RH), de acordo com suas características de manuseio de informações confidenciais e atividades consideradas críticas e ou vitais para o INR, devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

10.2.1 | Proteção contra Ameaças Externas

A vizinhança do INR e de suas áreas podem representar riscos para sua segurança. Temos como riscos: vizinhos que armazenem produtos inflamáveis, grande trânsito de pessoas no prédio, órgãos públicos no mesmo prédio e outros. Existem ainda outras ameaças que devem ser consideradas tais como: desastres naturais, incidentes de infraestrutura, incêndios, atentados e outros.

As ameaças externas devem ser avaliadas quanto ao risco para os negócios do INR e devem ser implantadas as medidas de proteção possíveis que se façam necessário. Caso não seja possível a eliminação dos riscos, um processo de continuidade de negócios deve ser implantado com planos de emergência, crises e recuperação de desastres.

10.2.2 | Segurança do Cabeamento

O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações devem ser protegidos contra interceptação, interferência ou danos. A documentação dos componentes da rede LAN (cabos e demais equipamentos) deve estar sempre atualizada e disponível para utilização em situação de necessidade.

10.3 | Segurança de Equipamentos e Ativos Fora do INR

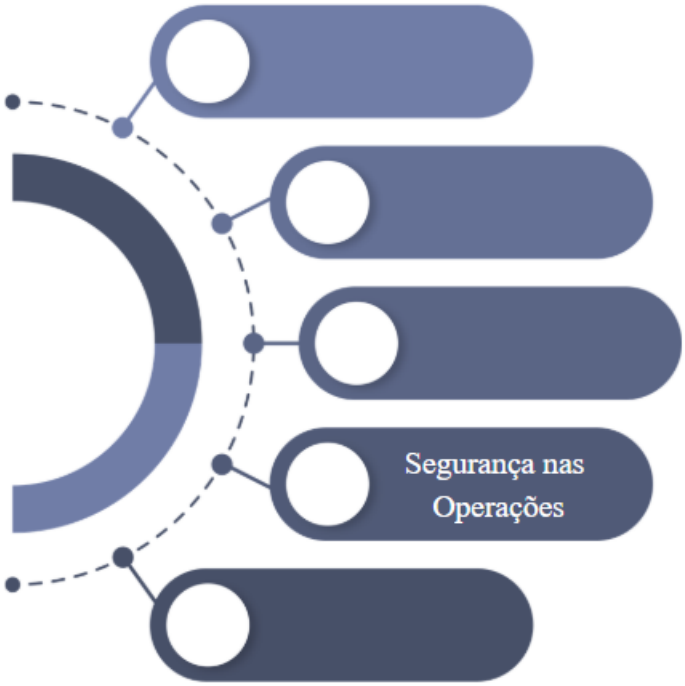
A maneira mais comum de usar o acesso remoto é por meio de uma VPN (Rede Privada Virtual), que consegue estabelecer uma ligação direta entre o computador e o servidor de destino, criando uma espécie de túnel protegido na Internet. Isto significa que o usuário pode acessar tranquilamente seus documentos, e-mails corporativos e sistemas na nuvem, via VPN, sem preocupação de ser interceptado por administradores de outras redes.

10.4 | Trabalho Remoto

Trabalho remoto ou *home office* significa literalmente, realizarmos determinadas atividades do dia a dia remotamente (em casa). O INR tem definido que em alguns dias da semana o trabalho de seus colaboradores será feito remotamente. Dessa forma, alguns cuidados devem ser considerados pelos colaboradores, tais como:

- Prover equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;
- Prover segurança física no local remoto de trabalho;
- Manter procedimentos para cópias de segurança e continuidade de negócios, devidamente armazenadas;
- Realizar auditoria e monitoramento de segurança;
- Devolver equipamento, quando as atividades de trabalho remoto se encerrarem; e
- Evitar a acesso de familiares e visitantes a equipamentos e informações que estão sendo utilizados remotamente.

11 | SEGURANÇA NAS OPERAÇÕES



O objetivo da segurança nas operações é fornecer direcionamentos para proteção das informações quanto a sua disponibilidade, confidencialidade e a integridade na utilização dos recursos de tecnologia da informação, cumprindo os regulamentos e requisitos legais, bem como os requisitos das agências reguladoras.

11.1 | Documentação dos Procedimentos Operacionais

Os processos e atividades operacionais de tecnologia da informação apresentam grande número de ações e complexidades específicas, que são um grande desafio para que seja conseguida a adequada continuidade operacional dos serviços. Dessa forma, existem alguns requisitos básicos que devem ser disponibilizados tais como: documentação dos procedimentos, metodologia adequada, treinamento e acompanhamento gerencial.

11.1.1 | Diretrizes e Controles

Os líderes e colaboradores do INR devem orientar e garantir o desenvolvimento, disponibilização e utilização de documentação para os procedimentos operacionais de sua área de atuação. Esses procedimentos devem ser simples, efetivos e estarem sempre atualizados.

Periodicamente, pelo menos semestralmente, o líder responsável pela área deve fazer uma avaliação da documentação existente, sua efetividade e treinamento para sua utilização.

11.1.2 | Avaliação e Auditoria

Os líderes do INR têm a responsabilidade por garantir:

- A existência de repositório com procedimentos operacionais documentados;
- A utilização adequada da documentação armazenada no repositório;
- Garantir treinamento para utilização da documentação existente no repositório; e
- Garantir orientações e cobranças sobre utilização do repositório e manutenções são realizadas com a frequência.

11.2 | Gerenciamento de Mudanças

O objetivo do gerenciamento de mudanças é propor e disponibilizar um processo que vai guiar a execução das mudanças de forma mais eficiente, reduzindo o impacto comercial, os custos e os riscos, que podem gerar a redução da estabilidade ou disponibilidade de TI.

O **Procedimento de Gerência de Mudanças** descreve em detalhe o processo de mudanças.

11.3 | Separação dos Ambientes de Produção e Outros

O ambiente operacional da área de tecnologia da informação, para garantir a sua segurança, exige que sejam adotadas estruturas independentes e isoladas entre os ambientes de produção e demais ambientes operacionais, evitando que devido a alguma falha os dados de produção sejam corrompidos (deletados, modificados, etc).

11.3.1 | Tipos de Ambientes Operacionais

- **Ambiente de Produção**: É o ambiente operacional utilizado para suportar as operações de produção do INR. Nesse ambiente é proibido executar testes e implantações.
- **Ambiente de Desenvolvimento**: É o ambiente operacional utilizado para suportar as operações de desenvolvimento de sistemas e / ou avaliação de sistemas adquiridos de terceiros. Nesse ambiente podemos: codificar, testar, errar e corrigir, sem afetar o ambiente de produção.
- **Ambiente de Teste**: As atividades de testes são elementos críticos para garantia da qualidade para a implantação de soluções no ambiente produtivo, sejam as desenvolvidas internamente ou adquiridas no mercado, principalmente quando customizadas. Os dados

utilizados nos testes são totalmente independentes dos dados de produção.

- **Ambiente de Homologação**: É o ambiente utilizado apenas para testes finais, que simula o ambiente de produção. Todos os documentos enviados a esse ambiente não possuem validade jurídica, podendo ser utilizado dados reais ou fictícios.

11.4 | Proteção contra Códigos Maliciosos (*Malware*)

A proteção contra códigos maliciosos tem como objetivo assegurar que as informações e os recursos de processamento da informação estarão protegidos adequadamente. Para manter os computadores livres da ação dos códigos maliciosos existe um conjunto de medidas preventivas que devem ser adotadas. Essas medidas incluem manter os programas instalados com as versões mais recentes e com todas as atualizações disponíveis aplicadas e utilização de mecanismos de segurança, como AntiMalware e firewall.

11.5 | Medidas de Segurança

Recomenda-se as-seguintes medidas para atender a segurança de informações:

- **Backup** (cópia de segurança): o backup dos dados e sistemas do INR deve ser executado conforme definido no Procedimento de Backup do INR;
- **Antivírus**: são softwares de monitoramento e combate à programas maliciosos que obrigatoriamente devem estar instalados nos servidores e nas estações de trabalho do INR;
- **Atualização Contínua**: é extremamente importante que o sistema operacional e seus componentes estejam atualizados. Softwares padrões como navegadores ou mesmo ferramentas do office podem conter falhas em sua programação o que abre vulnerabilidades para ataques diversos. Essas atualizações do sistema visam corrigir essas falhas à medida que estas são descobertas.
- **Engenharia Social**: é um método que consiste em persuadir a vítima estimulando confiança para obtenção de informações privilegiadas ou mesmo viabilizar que o alvo baixe um arquivo enviado ou acesse um link malicioso. O responsável pela segurança de informações deve conscientizar e dar todo suporte para os demais colaboradores do INR.

11.6 | Registros e Monitoramento

Arquivos de registro (logs) são vitais para a organização, pois são utilizados para ajudar na solução problemas de TI, investigar incidentes de segurança, atender a LGPD, localizar um erro de aplicativo ou isolar um componente de baixo desempenho.

11.6.1 | Proteção das Informações dos Registros de Eventos

O registro de logs tem como objetivo principal a detecção de ações impróprias nos sistemas de informação. Devem ser tomados cuidados para que esse monitoramento esteja de acordo com requisitos legais e preserve a salvo as informações pessoais e confidenciais.

11.7 | Orientações para o Ambiente Operacional

As instalações e manutenções de software operacional devem obedecer a alguns cuidados e procedimentos específicos que são listados a seguir:

- Ter um inventário de software, releases e versões instalados;
- Ter registro das Licenças de Software adquiridas pelo INR com as seguintes informações:
  - ✓ NF (nota fiscal);
  - ✓ Fornecedor;
  - ✓ Chave de ativação;
  - ✓ Análise das licenças adquiridas; e
  - ✓ Análise das licenças instaladas;
- Serem estudados e aprovados, pelos responsáveis pelos softwares e gerência de suporte;
- Serem aprovados pelo processo de Gerenciamento de Mudanças;
- Testados antes de disponibilização para produção;
- As mudanças devem ser documentadas e disponibilizada para serem usadas em caso de necessidade;
- Manter histórico de manutenções; e
- Devem ser considerados todos os direcionamentos relativos à norma de utilização de senhas.

11.8 | Avaliação e Auditoria

Além de avaliar a utilização da segurança de informações no INR, devem existir preocupação constante em garantir que existência de evidências para atender auditorias, garantindo o cumprimento dos seguintes itens:

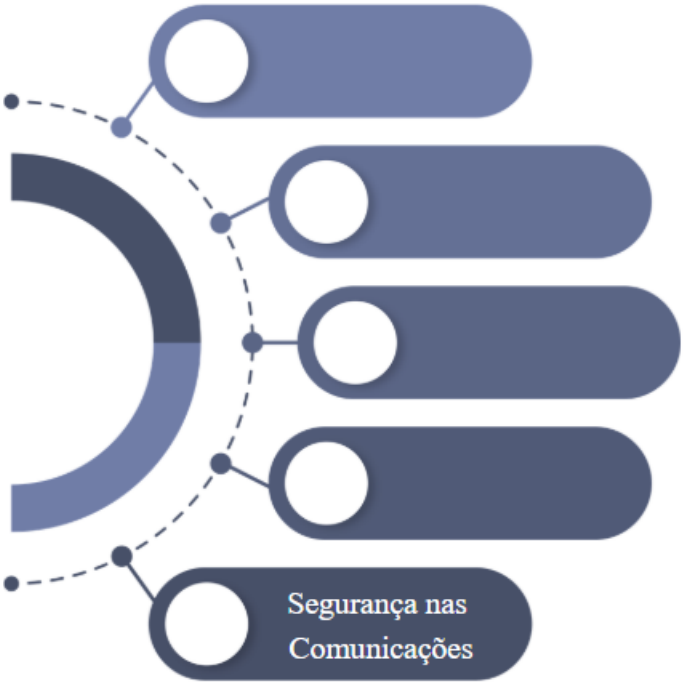
- Atender recomendações técnicas de instalações e atualizações de segurança de informações;
- Utilizar gerenciamento de mudanças, mantendo evidências;
- Garantir a existência de documentação demonstrando atendimentos dos requisitos de segurança; e
- Armazenar documentações relacionadas com incidentes ocorridos durante o ano.

11.9 | Auditoria de Sistemas

A auditoria de sistemas de informação visa verificar a conformidade não dos aspectos contábeis da organização, mas sim do próprio ambiente informatizado, garantindo a integridade dos dados manipulados pelo computador.

Assim, ela estabelece e mantém procedimentos documentados para planejamento e utilização dos recursos computacionais do INR, verificando aspectos de segurança e qualidade.

12 | SEGURANÇA NAS COMUNICAÇÕES



A segurança nas comunicações é um dos pilares da proteção da informação dentro de uma organização. Seu objetivo principal é garantir que os dados transmitidos, em qualquer meio — físico ou digital —, sejam protegidos contra interceptações, alterações, perdas ou acessos não autorizados.

Ao estabelecer diretrizes claras e procedimentos padronizados para o envio e recebimento de dados, o INR fortalece sua resiliência contra ameaças cibernéticas e reduz os riscos operacionais associados à exposição indevida de informações sensíveis.

12.1| Gerenciamento da Segurança em Redes e Internet

A área responsável pelas redes no INR mantém mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede. Os serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados. A seguir citamos os alguns desses componentes:

- **Firewall**
  Para ajudar a manter as redes mais seguras, os “Firewalls” remetem à ideia de uma única passagem para os dados, onde todos são analisados antes de serem liberados e, de fato, o que acontece é exatamente isso, todo o tráfego de uma rede passa obrigatoriamente por uma estação de controle para ser analisado, caso não encontre nenhuma restrição, o “Firewall” libera o pacote e este segue para seu destino, caso contrário, é sumariamente descartado. Normalmente, um “Firewall” é instalado no ponto de interligação de uma rede interna com a

Internet. Todo o tráfego, nos dois sentidos, deve passar por este ponto e, dessa forma, atender aos requisitos da política de segurança de comunicações.

- **Antivírus**
  Como é sabido, nenhum dos métodos disponíveis até hoje é completamente eficaz contra as pragas virtuais. O mais certo é utilizar um antivírus que esteja sempre atualizado e que possua métodos de detecção próprios eficientes como a Análise Heurística e a Checagem da Integridade, mesmo assim, deve-se sempre instalar softwares originais e de fontes confiáveis.

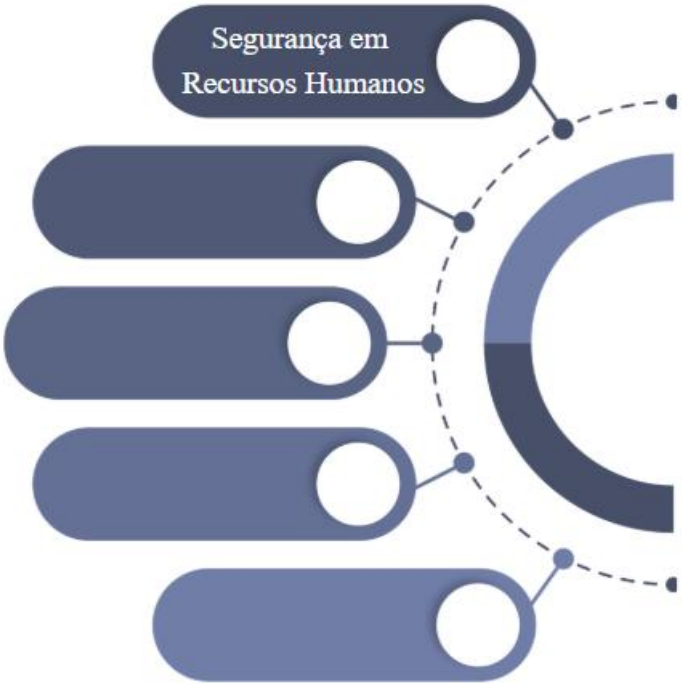
- **Segregação de Redes**
  O método de controlar a segurança da informação em grandes redes é dividi-la em domínios de redes lógicas diferentes, que garante acesso restrito a certos serviços.

12.2 | Monitoramento

O monitoramento das atividades em um ambiente de tecnologia da informação tem como objetivo principal detectar atividades não autorizadas realizadas por usuários internos ou externos. O registro das atividades deve ser feito de forma automática pelos sistemas, gerando um arquivo chamado de log. Este arquivo deve ser protegido contra falsificação e acesso não autorizado, mantendo a sua integridade e confiabilidade caso seja necessário utilizá-lo.

13 | SEGURANÇA NOS RECURSOS HUMANOS

A área de RH é responsável por contratar, organizar e guardar os dados pessoais de todos os colaboradores, bem como as informações de empresas prestadoras de serviços.



Os dados dos colaboradores são extremamente estratégicos, pois estão relacionados à força de trabalho e devem ser tratados como confidenciais e de acordo com as regulamentações/leis vigentes.

13.1| Segurança da Informação em RH

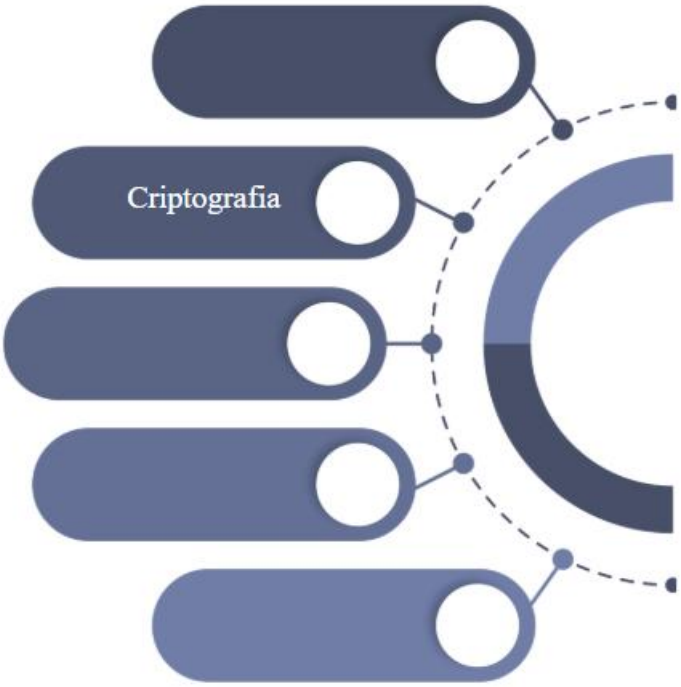
Apresentamos a seguir algumas orientações de ações conjuntas que vão otimizar a segurança da informação em RH:

- **Plano de conduta:** Devem ser documentados os processos e procedimentos de armazenamento e compartilhamento seguro dos dados, seguindo regras específicas do programa de segurança de informações, implantadas na INR.
- **Contratos de confidencialidade:** são medidas preventivas essenciais que devem serem adotadas para garantir a confidencialidade, autenticidade e disponibilidade dos dados de colaboradores e terceiros.
- **Treinamentos internos:** devem ser realizados para conscientizar os colaboradores sobre a importância da segurança da informação em RH. Os novos funcionários e terceiros contratados, devem receber treinamento para garantir o alinhamento com o programa de segurança de informações implantado.
- **Integração dos setores de RH e TI:** Os setores de RH e TI, devem estar cientes da necessidade de trabalhar em parceria para criar uma barreira blindada de proteção aos sistemas internos do INR.

- **Férias:** É vedado ao colaborador permanecer com equipamentos corporativos durante o período de férias, salvo autorização expressa, visando: segurança da informação; e mitigação de riscos trabalhistas.
- **Ferramenta MFA:** O segundo fator de autenticação será gerenciado pela área de TI, não sendo permitido uso em dispositivos pessoais dos usuários, como medida de controle e segurança.

14 | CRIPTOGRAFIA

A criptografia é um mecanismo essencial para a proteção da confidencialidade e integridade das informações sensíveis processadas, armazenadas ou transmitidas no ambiente do INR.



Sua aplicação visa garantir que apenas usuários autorizados tenham acesso ao conteúdo da informação, mesmo em caso de interceptação ou acesso indevido aos dados.

14.1 | Princípios e Diretrizes

A utilização de criptografia deve obedecer aos seguintes princípios e diretrizes:

- **Abrangência**: A criptografia deve ser aplicada em dados considerados sensíveis, confidenciais ou críticos, tanto em trânsito (comunicações eletrônicas) quanto em repouso (armazenamento local ou em nuvem);
- **Algoritmos e Padrões**: Devem ser utilizados algoritmos criptográficos reconhecidos por órgãos e padrões internacionais (ex.: AES, RSA, SHA-2), evitando o uso de tecnologias obsoletas ou vulneráveis;
- **Gestão de Chaves**: O processo de geração, distribuição, armazenamento, renovação e descarte de chaves criptográficas deve seguir procedimentos seguros e documentados, com segregação de funções e controle de acesso;
- **Criptografia em Comunicações**: É obrigatória a utilização de canais criptografados (ex.: HTTPS, VPN, TLS) para a troca de informações sensíveis com usuários internos, clientes, parceiros ou prestadores de serviços;

- **Criptografia de Dispositivos e Mídias**: Equipamentos móveis, dispositivos removíveis e mídias de backup que contenham dados sensíveis devem ser protegidos por criptografia;

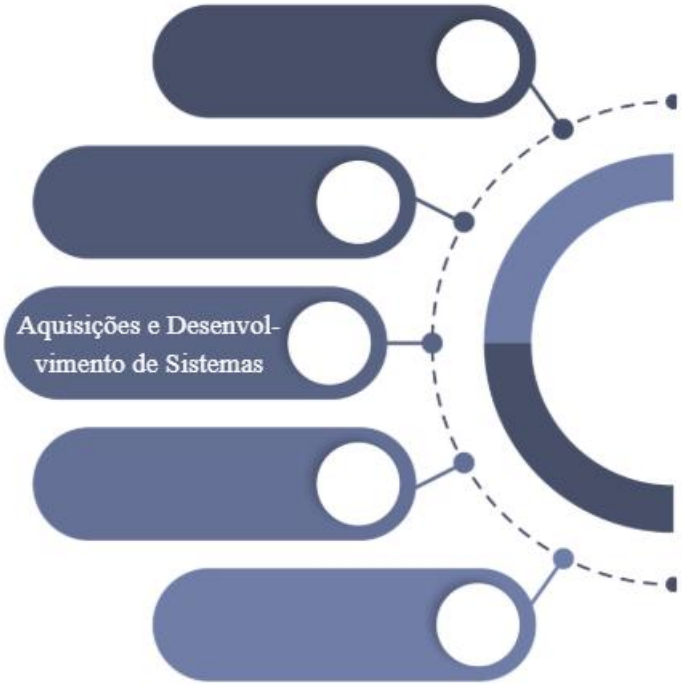
- **Adoção de Certificados Digitais**: Sempre que possível, devem ser adotados certificados digitais válidos, emitidos por autoridades certificadoras reconhecidas, para garantir a autenticidade das comunicações e transações;

- **Auditoria e Conformidade**: A aplicação da criptografia será periodicamente auditada para assegurar a conformidade com esta política e com as exigências legais e regulatórias vigentes.

A área responsável pela segurança da informação deve revisar periodicamente os métodos criptográficos adotados, visando sua atualização conforme a evolução tecnológica e os riscos emergentes.

15 | AQUISIÇÕES E DESENVOLVIMENTO DE SISTEMAS

A aquisição e desenvolvimento de sistemas define direcionamentos que devem nortear a aquisição, desenvolvimento e manutenção de sistemas de informação, visando assegurar a disponibilidade e continuidade dos serviços prestados por estes sistemas, minimizando os riscos ao negócio e atendimento dos requisitos de segurança de informações.



O **Procedimento de Aquisição e Desenvolvimento de Sistemas** descreve de forma completa esse processo.

15.1 | Aquisição de Sistemas

A aquisição de sistemas pelo INR deve observar critérios técnicos e de segurança da informação, de forma a garantir que os recursos contratados atendam aos requisitos de confidencialidade, integridade, disponibilidade e conformidade legal aplicáveis aos dados e processos institucionais.

15.1.1| Diretrizes para Aquisição de Sistemas

- **Requisitos de Segurança**: Todos os processos de aquisição de sistemas devem incluir, entre seus critérios de seleção, exigências específicas de segurança da informação, compatíveis com a criticidade das informações que serão tratadas pelo sistema;

- **Avaliação Técnica e Funcional**: Antes da contratação, deve ser realizada análise técnica para verificar se o sistema contempla mecanismos adequados de controle de acesso, autenticação, criptografia, registro de logs e proteção contra vulnerabilidades conhecidas;

- **Testes de Segurança**: Sempre que possível, o sistema a ser adquirido deve ser submetido a testes de segurança (ex.: análise de vulnerabilidades) antes da homologação e entrada em produção;

- **Cláusulas Contratuais de Segurança**: Os contratos com fornecedores devem prever cláusulas específicas relacionadas à proteção da informação, confidencialidade, responsabilidade em caso de falhas, suporte técnico e correção de vulnerabilidades;

- **Atualizações e Suporte**: Deve ser exigido do fornecedor o compromisso com a entrega de atualizações periódicas de segurança, correções de falhas e suporte técnico durante todo o ciclo de vida do sistema; e

- **Conformidade Legal e Regulatória**: O sistema adquirido deve estar em conformidade com a legislação vigente, incluindo, quando aplicável, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

16 | GESTÃO DE INCIDENTES E CONTINUIDADE DO NEGÓCIO

A gestão de incidentes de segurança da informação e a continuidade do negócio são elementos estratégicos para a resiliência operacional do INR. A ocorrência de falhas, ataques cibernéticos, indisponibilidades ou qualquer evento que comprometa a segurança das informações deve ser tratada de forma estruturada e eficiente, com o objetivo de minimizar impactos, restaurar os serviços afetados e preservar a integridade das operações institucionais.

A adoção de um processo formal de resposta a incidentes permite a identificação, registro, análise, tratamento e comunicação adequada de ocorrências que envolvam a segurança da informação. Da mesma forma, a continuidade do negócio exige a elaboração de planos específicos, com foco na retomada das atividades críticas dentro de prazos aceitáveis, garantindo a entrega dos serviços essenciais mesmo diante de situações adversas.

Nesse contexto, a atuação preventiva, a capacitação das equipes, a definição de responsabilidades e a realização periódica de testes e simulações são fundamentais para assegurar a eficácia das ações e a maturidade da gestão de riscos no ambiente organizacional.

16.1 | Gestão de Incidentes

A Gestão de Incidentes tem como objetivo:

- Garantir a detecção de eventos, execução de tratamento adequado para os incidentes de segurança;
- Minimizar os efeitos adversos de incidentes de segurança, tratando-os o mais brevemente possível;

- Reportar as vulnerabilidades de segurança da informação, além de tratá-las adequadamente;
- Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas; e
- Atender os requisitos da Lei Geral de Proteção de Dados (LGPD).

A **Política de Gestão de Resposta a Incidentes** descreve de forma completa esse processo.

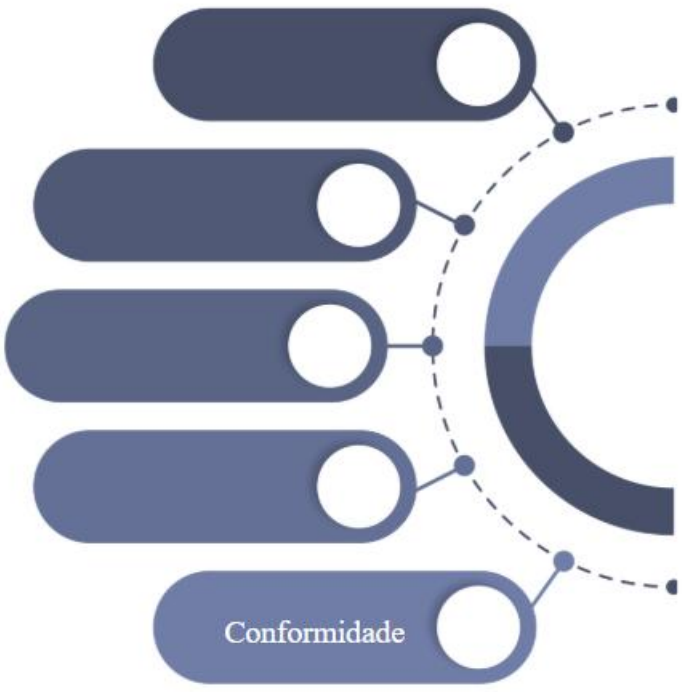
16.2 | Gestão de Continuidade de Negócios

O planejamento da gestão de continuidade de negócios do INR tem como objetivo disponibilizar direcionamentos e ações a serem executados no caso de ocorrência de incidentes e / ou desastres.

A **Política de Continuidade de Negócios** descreve os planos a serem utilizados para garantir a continuidade de negócios do INR.

17 | CONFORMIDADE

O objetivo da conformidade é mostrar regras e direcionamentos a serem utilizados no INR, para garantir sua aderência às leis, regulamentações, contratos, políticas e diretrizes estabelecidas.



17.1 | Diretrizes

Os líderes e demais colaboradores devem garantir que leis, regulamentações, políticas e diretrizes que envolvam segurança de informações e os negócios em geral, sejam adequadamente atendidas.

Garantir que eventuais desvios e inconformidades que possam ocorrer sejam evitadas, detectadas e tratadas dentro de um prazo razoável.

Líderes e demais colaboradores devem identificar possíveis desvios e executar ações para atender os requisitos de conformidade.

17.2 | Requisitos Legais e Contratuais

O INR está estruturado para atender todas as regras relativas à conformidade, ou seja, utiliza controles e proteções para evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, relacionadas com a segurança da informação e de quaisquer itens que possam afetar a qualidade e segurança dos serviços do INR.

17.3 | Identificação e Requisitos

Os líderes e colaboradores do INR, em qualquer situação que envolva atendimento ou conformidades em geral, devem executar as seguintes ações:

- Entender os requisitos: buscar o máximo de informações sobre o assunto em questão;
- Criar políticas internas: documentar a forma de atuação em relação ao requisito;
- Analisar os riscos: verificar os riscos envolvidos na situação e na decisão tomada;
- Documentar os resultados: após a análise devem ser documentadas desvios e as recomendações de melhorias; e
- Tratar os desvios: aplicar ações no sentido de eliminar ou atenuar os desvios identificados.

17.4 | Proteção de Registros

A segurança de informações com suas políticas, diretrizes, normas e procedimentos visam proteger os registros de informações do INR, dos colaboradores, parceiros, fornecedores e clientes contra qualquer forma de acesso ou utilização indevida.

Essa proteção visa atender as legislações existentes que definem o porquê e como proteger os ativos de informação, incluindo a Lei Geral de Proteção de Dados (LGPD).

Os líderes e os colaboradores são responsáveis por implantar controles e proteções contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.