POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



PSI-001

Allcance Soluções em Tecnologia LTDA. CNPJ: 13.293.239/0001-49

Endereço: Rua Rio Jurema, nº 47, Bairro Nossa Senhora das Graças, na Cidade de Manaus, Estado de Amazonas

Website: www.allcance.tec.br

Controle de Documento

Título do Documento	Política de Segurança da Informação
Código do Documento	PSI-001
Versão	2.0
Status	Aprovado
Data de Publicação	15 de Março de 2025
Aprovado por	Diretoria Executiva
Próxima Revisão	15 de Março de 2026

Sumário Executivo

Esta Política de Segurança da Informação (PSI) estabelece o compromisso da Allcance Soluções com a proteção de seus ativos de informação. O documento define as diretrizes técnicas e operacionais para garantir a confidencialidade, integridade e disponibilidade das informações, abrangendo desde a gestão de incidentes e continuidade de negócios até o uso seguro de dispositivos pessoais. O objetivo é mitigar riscos, assegurar a conformidade e proteger a reputação da empresa, estabelecendo um framework robusto de segurança para todos os colaboradores e parceiros.

Sumário

Sumário Executivo 3
1. Política de Segurança da Informação 7
1.1 Objetivo 7
1.2. Escopo 7
1.3 Princípios da Segurança da Informação 7
1.4 Diretrizes Gerais 7
1.4.1 Gestão de Ativos da Informação 7
1.4.2 Gestão de Acessos 8
1.4.3 Segurança Física e do Ambiente 8
1.4.4 Segurança nas Operações 8
1.4.5 Segurança nas Comunicações 8
1.4.6 Aquisição, Desenvolvimento e Manutenção de Sistemas 8
1.4.7 Gestão de Incidentes de Segurança da Informação 8
1.4.8 Continuidade de Negócios 9
1.4.9 Conformidade 9
1.5 Responsabilidades 9
1.6 Conscientização e Treinamento 9
1.7 Gestão de Consequências 9
1.8. Documentos Complementares 9
1.9. Revisão da Política 10
2. Política de Tratamento de Incidentes de Segurança 11
2.1 Objetivo 11
2.2 Escopo 11
2.3 Definições 11
2.4 Estrutura de Resposta a Incidentes 11
2.4.1 Equipe de Resposta a Incidentes de Segurança (ERIS) 11
2.4.2 Classificação de Incidentes 12
2.5 Fases do Processo de Gestão de Incidentes 12
2.6 Comunicação de Incidentes com Dados Pessoais 13
2.7 Responsabilidades 14
2.8 Revisão da Política 14

3. Política de Continuidade de Negócios 15
3.1 Objetivo 15
3.2 Escopo 15
3.3 Estrutura de Gestão da Continuidade de Negócios 15
3.3.1 Análise de Impacto no Negócio (BIA - Business Impact Analysis) 15
3.3.2 Avaliação de Riscos 15
3.3.3 Estratégias de Continuidade e Recuperação 15
3.3.4 Plano de Continuidade de Negócios (PCN) 16
3.4 Testes e Exercícios 16
3.5 Treinamento e Conscientização 16
3.6 Revisão e Melhoria Contínua 16
3.7 Responsabilidades 17
3.8 Documentos Complementares 17
4. Política de Backup e Recuperação 18
4.1 Objetivo 18
4.2 Escopo 18
4.3 Diretrizes de Backup 18
4.3.1 Identificação e Classificação de Dados 18
4.3.2 Estratégia de Backup 18
4.3.3 Armazenamento e Retenção 18
4.3.4 Criptografia 19
4.4 Diretrizes de Recuperação 19
4.4.1 Plano de Recuperação 19
4.4.2 Testes de Recuperação 19
4.5 Monitoramento e Gerenciamento 19
4.6 Responsabilidades 20
4.7 Revisão da Política 20
5. Política de Uso de Dispositivos Pessoais (BYOD) 21
12.1 Objetivo 21
5.2 Escopo 21
5.3 Diretrizes Gerais 21
5.3.1 Elegibilidade e Registro 21
5.3.2 Requisitos Mínimos de Segurança do Dispositivo 21
5.3.3 Acesso à Rede e aos Dados 22

5.4 Responsabilidades do Usuário 22
5.5 Direitos da Allcance Soluções 22
5.6 Privacidade 23
5.7 Término do Acesso 23
5.8 Sanções 23
6. Glossário de Termos 24

1. Política de Segurança da Informação

1.1 Objetivo

Esta Política de Segurança da Informação (PSI) tem como objetivo estabelecer as diretrizes e responsabilidades para proteger os ativos de informação da **Allcance Soluções** contra ameaças, garantindo a confidencialidade, integridade e disponibilidade das informações e assegurando a continuidade dos negócios, a conformidade legal e a proteção da reputação da empresa.

1.2. Escopo

Esta política se aplica a todos os colaboradores, diretores, conselheiros, prestadores de serviço, parceiros de negócio e quaisquer terceiros que tenham acesso a informações ou utilizem os recursos de tecnologia da informação da Allcance Soluções, independentemente de sua localização física ou vínculo contratual.

1.3 Princípios da Segurança da Informação

A segurança da informação na Allcance Soluções é fundamentada nos seguintes princípios:

- **Confidencialidade:** A informação deve ser acessível apenas por pessoas autorizadas. Medidas devem ser implementadas para prevenir a divulgação não autorizada de informações sensíveis.
- **Integridade:** A informação deve ser mantida em seu estado original, exata e completa, protegida contra alterações indevidas, não autorizadas ou acidentais.
- **Disponibilidade:** A informação e os sistemas associados devem estar disponíveis para os usuários autorizados sempre que necessário para a execução de suas atividades de negócio.
- **Autenticidade:** Garantir que a identidade de um usuário, sistema ou informação é genuína e pode ser verificada.
- **Não-repúdio (Irretratabilidade):** Garantir que uma ação ou transação não possa ser negada posteriormente por nenhuma das partes envolvidas.
- **Responsabilidade (Accountability):** Todas as ações realizadas em sistemas da Allcance Soluções devem ser rastreáveis a um indivíduo ou entidade específica.

1.4 Diretrizes Gerais

1.4.1 Gestão de Ativos da Informação

- **Inventário e Classificação:** Todos os ativos de informação (documentos, dados, sistemas, etc.) devem ser inventariados e classificados de acordo com seu nível de criticidade e sensibilidade (Público, Interno, Confidencial, Restrito). A responsabilidade pela classificação é do proprietário da informação.
- **Manuseio da Informação:** A informação deve ser manuseada de acordo com sua classificação, com controles específicos para armazenamento, transmissão, descarte e acesso.

1.4.2 Gestão de Acessos

- **Princípio do Menor Privilégio:** O acesso a sistemas e informações deve ser concedido com base na necessidade de negócio (need-to-know) e limitado ao mínimo necessário para a execução das funções do colaborador (least privilege).
- **Controle de Acesso Lógico:** O acesso a sistemas deve ser controlado por meio de identificação única e intransferível (login individual) e senhas fortes. A autenticação de múltiplos fatores (MFA) deve ser implementada em sistemas críticos.
- **Revisão de Acessos:** Os direitos de acesso devem ser revisados periodicamente (no mínimo, semestralmente) e revogados imediatamente após o término do vínculo do colaborador ou prestador de serviço.

1.4.3 Segurança Física e do Ambiente

- **Controle de Acesso Físico:** O acesso a áreas restritas, como data centers e salas de servidores, deve ser controlado e monitorado.
- **Proteção de Equipamentos:** Equipamentos de TI devem ser protegidos contra acesso não autorizado, roubo, danos e interferências ambientais.

1.4.4 Segurança nas Operações

- **Proteção contra Malware:** Todos os computadores e servidores devem possuir software de antivírus corporativo, mantido sempre atualizado.
- **Backup e Recuperação:** Devem existir procedimentos de backup e recuperação de dados para todas as informações críticas, com testes periódicos para garantir sua eficácia.
- **Gestão de Vulnerabilidades:** A empresa deve manter um processo contínuo para identificar, avaliar e tratar vulnerabilidades técnicas em seus sistemas e redes.

1.4.5 Segurança nas Comunicações

- **Segurança de Redes:** As redes de comunicação devem ser protegidas por firewalls e outras medidas de segurança para prevenir acessos não autorizados.
- **Transferência de Informações:** A transferência de informações confidenciais ou restritas deve ser feita por meios seguros e criptografados.

1.4.6 Aquisição, Desenvolvimento e Manutenção de Sistemas

- **Desenvolvimento Seguro:** Requisitos de segurança devem ser integrados ao ciclo de vida de desenvolvimento de software (SDLC).
- **Ambientes Separados:** Ambientes de desenvolvimento, teste e produção devem ser mantidos separados e com controles de acesso distintos.

1.4.7 Gestão de Incidentes de Segurança da Informação

- **Detecção e Resposta:** A Allcance Soluções deve manter um processo formal para detectar, relatar, avaliar e responder a incidentes de segurança da informação de forma rápida e eficaz.
- **Comunicação:** Incidentes que envolvam dados pessoais devem seguir o fluxo de comunicação estabelecido na Política de Privacidade e Proteção de Dados,

incluindo a notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, quando aplicável.

1.4.8 Continuidade de Negócios

- **Planejamento:** A empresa deve desenvolver e manter um Plano de Continuidade de Negócios (PCN) para garantir a recuperação e restauração de processos críticos de negócio em caso de desastres ou interrupções graves.

1.4.9 Conformidade

- **Requisitos Legais e Contratuais:** A Allcance Soluções deve identificar e cumprir todos os requisitos legais, regulatórios e contratuais aplicáveis à segurança da informação, incluindo a Lei Geral de Proteção de Dados (LGPD).
- **Auditorias:** Auditorias internas e externas de segurança da informação devem ser realizadas periodicamente para avaliar a conformidade com esta política e outras normas aplicáveis.

1.5 Responsabilidades

- **Diretoria Executiva:** Prover os recursos necessários e o apoio estratégico para a implementação e manutenção do programa de segurança da informação.
- **Gestor de Segurança da Informação (CISO/Responsável):** Coordenar a implementação desta política, gerenciar o programa de segurança, monitorar ameaças e reportar à diretoria.
- **Proprietários da Informação:** Classificar os ativos de informação sob sua responsabilidade e definir os requisitos de acesso.
- **Colaboradores e Terceiros:** Cumprir as diretrizes desta política e de seus documentos complementares, zelar pela segurança dos ativos de informação que utilizam e reportar quaisquer incidentes de segurança.

1.6 Conscientização e Treinamento

Todos os colaboradores devem receber treinamento sobre segurança da informação no momento da contratação e, posteriormente, de forma periódica (no mínimo, anualmente). O treinamento deve abordar as políticas, procedimentos e as responsabilidades individuais de cada um.

1.7 Gestão de Consequências

A violação desta política ou de seus normativos complementares por parte de colaboradores ou terceiros poderá resultar em sanções disciplinares, incluindo advertência, suspensão, demissão por justa causa ou rescisão contratual, sem prejuízo das medidas legais cabíveis na esfera cível e criminal.

1.8. Documentos Complementares

Esta política é complementada por um conjunto de normas e procedimentos específicos, incluindo, mas não se limitando a:

- Política de Privacidade e Proteção de Dados (PPD-001)

- Política de Classificação da Informação
- Política de Gestão de Acessos (PGA-001)
- Política de Backup e Recuperação (PBR-001)
- Política de Tratamento de Incidentes de Segurança (PTIS-001)
- Política de Continuidade de Negócios (PCN-001)
- Política de Gestão de Riscos (PGR-001)

1.9. Revisão da Política

Esta política será revisada anualmente ou sempre que ocorrerem mudanças significativas no ambiente de negócio, tecnológico ou regulatório que a afetem.

2. Política de Tratamento de Incidentes de Segurança

2.1 Objetivo

Esta política tem como objetivo estabelecer um processo estruturado e eficaz para a gestão de incidentes de segurança da informação na **Allcance Soluções**. O propósito é garantir uma resposta rápida e coordenada para detectar, conter, erradicar e se recuperar de incidentes, minimizando os impactos operacionais, financeiros e de reputação, e assegurando a conformidade com os requisitos legais, especialmente no que tange a incidentes envolvendo dados pessoais.

2.2 Escopo

Esta política se aplica a todos os colaboradores, prestadores de serviço e terceiros da Allcance Soluções, e abrange qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação, dados ou redes da empresa. Isso inclui, mas não se limita a, acessos não autorizados, vazamento de dados, ataques de malware (vírus, ransomware), negação de serviço (DoS/DDoS) e violações de políticas de segurança.

2.3 Definições

- **Evento de Segurança:** Qualquer ocorrência observada em um sistema ou rede que indique uma possível violação da política de segurança, falha de salvaguardas ou uma situação previamente desconhecida que possa ser relevante para a segurança.
- **Incidente de Segurança da Informação:** Um ou uma série de eventos de segurança indesejados ou inesperados, que tenham uma probabilidade significativa de comprometer as operações de negócio e ameaçar a segurança da informação (confidencialidade, integridade ou disponibilidade).
- **Incidente com Dados Pessoais:** Qualquer incidente de segurança que resulte, de modo acidental ou ilícito, na destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais.
- **Equipe de Resposta a Incidentes de Segurança (ERIS):** Grupo de pessoas com papéis e responsabilidades designados para responder a incidentes de segurança. Também conhecido como CSIRT (Computer Security Incident Response Team).

2.4 Estrutura de Resposta a Incidentes

2.4.1 Equipe de Resposta a Incidentes de Segurança (ERIS)

A Allcance Soluções manterá uma ERIS formalmente designada, composta por membros das seguintes áreas:

- **Líder da ERIS (Gestor de SI / CISO):** Coordena todas as ações de resposta.
- **Encarregado de Proteção de Dados (DPO):** Avalia o impacto sobre dados pessoais e orienta sobre as obrigações da LGPD.
- **TI / Infraestrutura:** Responsável pela análise técnica, contenção e erradicação da ameaça.

- **Jurídico:** Fornece orientação legal e avalia as implicações contratuais e regulatórias.
- **Comunicação / Marketing:** Gerencia a comunicação interna e externa, se necessário.
- **Recursos Humanos:** Lida com incidentes envolvendo colaboradores.

2.4.2 Classificação de Incidentes

Os incidentes serão classificados com base em seu impacto potencial e urgência, para priorizar a resposta. A classificação inicial será:

- **Crítico:** Impacto severo nos negócios, na reputação, nas finanças ou risco de dano relevante aos titulares de dados. Exige resposta imediata.
- **Alto:** Impacto significativo, mas limitado. Exige resposta urgente.
- **Médio:** Impacto moderado, afetando um número limitado de usuários ou sistemas. Exige resposta em tempo hábil.
- **Baixo:** Impacto mínimo, sem afetar a continuidade dos negócios ou a segurança de dados sensíveis.

2.5 Fases do Processo de Gestão de Incidentes

O ciclo de vida de um incidente será gerenciado através das seguintes fases:

Fase 1: Preparação

- **Prevenção:** Implementação de controles de segurança (firewalls, antivírus, etc.), gestão de vulnerabilidades e treinamentos de conscientização.
- **Planejamento:** Manutenção e revisão desta política e dos planos de resposta.
- **Ferramentas:** Disponibilização de ferramentas para detecção, análise e registro de incidentes.

Fase 2: Identificação e Notificação

- **Detecção:** Monitoramento contínuo de sistemas e redes para identificar eventos de segurança.
- **Notificação:** Qualquer colaborador ou terceiro que identifique um evento ou suspeita de incidente **DEVE** reportá-lo **IMEDIATAMENTE** através dos seguintes canais:
  - **E-mail:** seguranca@allcancesolucoes.net.br
  - **Telefone:** [Número de Telefone de Emergência de TI]
- **Registro:** Todo incidente reportado será registrado em um sistema de controle, com informações como data, hora, descrição, e quem reportou.

Fase 3: Contenção

- **Análise Inicial:** A ERIS realiza uma análise preliminar para confirmar a ocorrência do incidente e classificar sua severidade.

- **Estratégia de Contenção:** Definir a estratégia para limitar o dano e prevenir a propagação do incidente. Isso pode incluir isolar sistemas da rede, desativar contas de usuário comprometidas ou bloquear tráfego de IPs maliciosos.
- **Preservação de Evidências:** Coletar e preservar todas as evidências relacionadas ao incidente (logs, imagens de disco, etc.) para análise forense e para fins legais.

Fase 4: Erradicação

- **Análise da Causa Raiz:** Investigar o incidente para identificar a causa raiz e a extensão do comprometimento.
- **Remoção da Ameaça:** Eliminar completamente o componente malicioso do ambiente (ex: remover malware, corrigir vulnerabilidades exploradas).

Fase 5: Recuperação

- **Restauração dos Sistemas:** Restaurar os sistemas e dados afetados a partir de backups seguros e validados.
- **Monitoramento:** Aumentar o monitoramento dos sistemas recuperados para garantir que a ameaça foi completamente eliminada e que o sistema está funcionando normalmente.
- **Validação:** Confirmar com os proprietários dos processos de negócio que os sistemas estão operacionais e seguros.

Fase 6: Pós-Incidente (Lições Aprendidas)

- **Relatório Final:** Elaborar um relatório detalhado sobre o incidente, incluindo a cronologia dos eventos, o impacto, as ações tomadas e a causa raiz.
- **Reunião de Lições Aprendidas:** A ERIS se reunirá para revisar o incidente e a resposta, identificando pontos fortes e fracos no processo.
- **Plano de Melhoria:** Desenvolver um plano de ação para implementar melhorias nos controles, processos e políticas de segurança, a fim de prevenir a recorrência do incidente.

2.6 Comunicação de Incidentes com Dados Pessoais

Conforme a LGPD, no caso de um incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais, a Allcance Soluções, sob orientação do DPO e do Jurídico, tomará as seguintes ações:

1. **Comunicação à ANPD:** Notificar a Autoridade Nacional de Proteção de Dados em um prazo razoável, a partir do conhecimento do incidente. A comunicação deverá conter, no mínimo:
    - A descrição da natureza dos dados pessoais afetados.
    - As informações sobre os titulares envolvidos.
    - A indicação das medidas técnicas e de segurança utilizadas.
    - Os riscos relacionados ao incidente.
    - Os motivos da demora, em caso de comunicação tardia.

   – As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
2. **Comunicação aos Titulares:** Comunicar os titulares de dados afetados sobre a ocorrência do incidente, fornecendo as informações necessárias sobre o ocorrido e as medidas que estão sendo tomadas.

2.7 Responsabilidades

- **Todos os Colaboradores:** Têm a responsabilidade de estar cientes dos procedimentos de notificação e de reportar imediatamente qualquer suspeita de incidente de segurança.
- **ERIS:** É responsável por executar o processo de resposta a incidentes conforme descrito nesta política.
- **Gestores de Áreas de Negócio:** Devem colaborar com a ERIS durante a investigação e recuperação de incidentes que afetem seus processos.

2.8 Revisão da Política

Esta política será revisada anualmente ou após a ocorrência de um incidente crítico, para garantir sua contínua adequação e eficácia.

3. Política de Continuidade de Negócios

3.1 Objetivo

Esta Política de Continuidade de Negócios (PCN) tem como objetivo estabelecer as diretrizes e a estrutura de governança para garantir que a **Allcance Soluções** possa responder, recuperar, retomar e restaurar suas operações críticas de negócio a um nível predefinido, após a ocorrência de uma interrupção ou desastre. O foco é minimizar os impactos financeiros, operacionais, legais e de reputação, protegendo o bem-estar dos colaboradores, a confiança dos clientes e o valor da marca.

3.2 Escopo

Esta política se aplica a todos os processos de negócio, sistemas de informação, infraestrutura, colaboradores e localidades da Allcance Soluções. Ela orienta o desenvolvimento, implementação, teste e manutenção do Programa de Gestão de Continuidade de Negócios (PGCN) em toda a organização.

3.3 Estrutura de Gestão da Continuidade de Negócios

3.3.1 Análise de Impacto no Negócio (BIA - Business Impact Analysis)

A Allcance Soluções realizará periodicamente uma Análise de Impacto no Negócio (BIA) para identificar os processos de negócio críticos e os recursos que os suportam. A BIA determinará:

- **Tempo Objetivo de Recuperação (RTO - Recovery Time Objective):** O tempo máximo aceitável para que um processo de negócio seja restaurado após uma interrupção.
- **Ponto Objetivo de Recuperação (RPO - Recovery Point Objective):** A quantidade máxima de perda de dados que pode ser tolerada, medida em tempo.

3.3.2 Avaliação de Riscos

Uma avaliação de riscos será conduzida para identificar as ameaças internas e externas que podem causar interrupções nos processos de negócio (ex: falhas de energia, desastres naturais, ataques cibernéticos, pandemias). Para cada ameaça, serão avaliadas a probabilidade de ocorrência e o impacto potencial.

3.3.3 Estratégias de Continuidade e Recuperação

Com base nos resultados da BIA e da avaliação de riscos, serão desenvolvidas e implementadas estratégias para garantir a continuidade e a recuperação das operações. As estratégias podem incluir:

- **Pessoas:** Planos de sucessão, treinamento cruzado e modelos de trabalho remoto.
- **Instalações:** Acordos para locais de trabalho alternativos (sites de recuperação).

- **Tecnologia:** Soluções de alta disponibilidade, redundância de sistemas e planos de recuperação de desastres (Disaster Recovery) para a infraestrutura de TI.
- **Fornecedores:** Identificação de fornecedores alternativos para produtos e serviços críticos.

3.3.4 Plano de Continuidade de Negócios (PCN)

Serão desenvolvidos Planos de Continuidade de Negócios detalhados para as áreas críticas da empresa. Cada plano deverá conter, no mínimo:

- **Equipes de Gerenciamento de Crise:** Definição de papéis e responsabilidades.
- **Procedimentos de Ativação do Plano:** Critérios claros para declarar um desastre e ativar o plano.
- **Planos de Comunicação:** Estratégias para comunicação com colaboradores, clientes, mídia e outras partes interessadas.
- **Procedimentos de Recuperação:** Passos detalhados para recuperar os processos de negócio e a tecnologia de suporte.

3.4 Testes e Exercícios

Os Planos de Continuidade de Negócios serão testados regularmente para garantir sua eficácia e para que as equipes de resposta estejam preparadas. Os tipos de testes incluem:

- **Testes de Mesa (Tabletop):** Simulações baseadas em discussão de cenários de desastre.
- **Testes Funcionais:** Testes práticos de componentes específicos do plano (ex: restauração de backups).
- **Testes Completos:** Simulação em larga escala de um cenário de desastre, envolvendo a ativação completa do plano.

Os resultados de todos os testes serão documentados, e quaisquer lacunas ou falhas identificadas darão origem a planos de ação para melhoria.

3.5 Treinamento e Conscientização

Todos os colaboradores com responsabilidades no PCN receberão treinamento específico sobre seus papéis. Programas de conscientização serão realizados para garantir que todos na organização entendam a importância da continuidade dos negócios e seus deveres em caso de crise.

3.6 Revisão e Melhoria Contínua

O Programa de Gestão de Continuidade de Negócios será revisado e atualizado anualmente, ou sempre que ocorrerem mudanças significativas na organização (novos processos, sistemas, etc.) ou após a realização de testes e exercícios. Este ciclo de revisão garante que o programa permaneça relevante e eficaz.

3.7 Responsabilidades

- **Diretoria Executiva:** Patrocinar o PGCN, aprovar esta política e garantir a alocação de recursos necessários.
- **Gestor de Continuidade de Negócios:** Coordenar o desenvolvimento, implementação e manutenção do PGCN em toda a empresa.
- **Proprietários de Processos de Negócio:** Participar da BIA, definir os requisitos de recuperação para suas áreas e colaborar no desenvolvimento e teste dos planos.
- **Equipes de Gerenciamento de Crise:** Assumir a liderança durante um evento de interrupção, executando os planos conforme definido.

3.8 Documentos Complementares

- Análise de Impacto no Negócio (BIA)
- Avaliação de Riscos
- Plano de Recuperação de Desastres de TI (PRD-TI)
- Planos de Comunicação de Crise

4. Política de Backup e Recuperação

4.1 Objetivo

Esta política tem como objetivo estabelecer as diretrizes e os requisitos para a execução de cópias de segurança (backups) e a recuperação de dados e sistemas da **Allcance Soluções**. O propósito é garantir que as informações críticas para o negócio possam ser restauradas de forma íntegra e oportuna em caso de falha, corrupção de dados, ataque cibernético ou qualquer outro evento que resulte em perda de dados, suportando assim a continuidade das operações e os objetivos de recuperação definidos na Política de Continuidade de Negócios.

4.2 Escopo

Esta política se aplica a todos os dados e sistemas de informação críticos para os negócios da Allcance Soluções, incluindo, mas não se limitando a, servidores, bancos de dados, sistemas de arquivos, aplicações e configurações de rede, independentemente de estarem hospedados em ambiente local (on-premises) ou em nuvem (cloud).

4.3 Diretrizes de Backup

4.3.1 Identificação e Classificação de Dados

- Todos os dados e sistemas devem ser classificados de acordo com sua criticidade para o negócio, conforme a Análise de Impacto no Negócio (BIA). Esta classificação determinará a frequência, o tipo e o período de retenção dos backups.
- Os requisitos de **RPO (Recovery Point Objective)**, definidos na BIA, serão a base para a definição da frequência dos backups de cada sistema.

4.3.2 Estratégia de Backup

- **Tipos de Backup:** Serão utilizados diferentes tipos de backup para otimizar o tempo e o espaço de armazenamento, incluindo:
  - **Backup Completo (Full):** Cópia de todos os dados selecionados. Será executado semanalmente para a maioria dos sistemas.
  - **Backup Incremental ou Diferencial:** Cópia apenas dos dados alterados desde o último backup (completo ou incremental). Será executado diariamente.
- **Frequência:** A frequência dos backups será definida com base no RPO de cada sistema, garantindo a mínima perda de dados possível.
- **Agendamento:** Os backups serão agendados para ocorrerem preferencialmente fora do horário de pico de produção, para minimizar o impacto no desempenho dos sistemas.

4.3.3 Armazenamento e Retenção

- **Regra 3-2-1:** A estratégia de armazenamento seguirá a regra 3-2-1 como boa prática:

  - Manter pelo menos **três** cópias dos dados.
  - Armazenar as cópias em **dois** tipos de mídia diferentes.
  - Manter **uma** cópia fora da localidade principal (off-site), preferencialmente em nuvem ou em um local geograficamente distinto.
- **Segurança das Mídias:** As mídias de backup, físicas ou virtuais, devem ser protegidas com controles de acesso e criptografia para prevenir acesso não autorizado, roubo ou perda.
- **Período de Retenção:** O período de retenção dos backups será definido com base em requisitos de negócio, legais e regulatórios. Ao final do período, as mídias serão descartadas ou sobrescritas de forma segura.

4.3.4 Criptografia

- Todos os backups de dados classificados como Confidenciais ou Restritos **devem** ser criptografados, tanto em trânsito (durante a transmissão para o local de armazenamento) quanto em repouso (no armazenamento final).

4.4 Diretrizes de Recuperação

4.4.1 Plano de Recuperação

- Devem existir procedimentos de recuperação documentados para cada sistema crítico, detalhando o passo a passo para a restauração dos dados e do ambiente a partir dos backups.
- Os requisitos de **RTO (Recovery Time Objective)**, definidos na BIA, guiarão a priorização da recuperação dos sistemas.

4.4.2 Testes de Recuperação

- Testes de recuperação (restauração) **devem** ser realizados periodicamente (no mínimo, semestralmente) para validar a integridade dos backups e a eficácia dos procedimentos de recuperação.
- Os testes devem simular cenários de falha realistas e os resultados devem ser documentados, incluindo o tempo real de recuperação e quaisquer problemas encontrados.
- Falhas nos testes de restauração devem ser tratadas com a máxima prioridade.

4.5 Monitoramento e Gerenciamento

- **Monitoramento:** O processo de backup deve ser monitorado diariamente para garantir que as rotinas sejam concluídas com sucesso. Alertas automáticos devem ser configurados para notificar a equipe de TI sobre quaisquer falhas.
- **Relatórios:** Relatórios sobre o status dos backups (sucessos, falhas, volume de dados, etc.) devem ser gerados e revisados regularmente pela equipe de TI.
- **Gestão de Capacidade:** O espaço de armazenamento para backups deve ser monitorado e planejado para garantir que haja capacidade suficiente para atender às políticas de retenção.

4.6 Responsabilidades

- **Gestor de TI:** Responsável por garantir a implementação, operação e monitoramento do processo de backup e recuperação, em conformidade com esta política.
- **Equipe de TI:** Responsável por executar as rotinas de backup, realizar os testes de recuperação e responder a incidentes de perda de dados.
- **Proprietários de Sistemas/Dados:** Responsáveis por informar à TI sobre novos sistemas ou mudanças na criticidade dos dados para que sejam incluídos na rotina de backup.

4.7 Revisão da Política

Esta política será revisada anualmente ou sempre que ocorrerem mudanças significativas na infraestrutura de TI ou nos requisitos de negócio, para garantir sua contínua adequação e eficácia.

5. Política de Uso de Dispositivos Pessoais (BYOD)

12.1 Objetivo

Esta política tem como objetivo estabelecer as diretrizes e os requisitos de segurança para o uso de dispositivos pessoais (como smartphones, tablets e laptops), uma prática conhecida como BYOD (Bring Your Own Device), para acessar recursos corporativos, redes e informações da **Allcance Soluções**. O propósito é equilibrar a flexibilidade e a produtividade dos colaboradores com a necessidade de proteger os ativos de informação da empresa e garantir a conformidade com as políticas de segurança e privacidade.

5.2 Escopo

Esta política se aplica a todos os colaboradores, prestadores de serviço e terceiros autorizados que utilizam seus dispositivos pessoais para se conectar à rede corporativa, acessar e-mails, sistemas de informação ou armazenar dados da Allcance Soluções, independentemente de estarem trabalhando nas instalações da empresa ou remotamente.

5.3 Diretrizes Gerais

5.3.1 Elegibilidade e Registro

- O uso de dispositivos pessoais para fins corporativos é um privilégio, não um direito, e pode ser revogado pela Allcance Soluções a qualquer momento.
- Todo dispositivo pessoal que será utilizado para acessar recursos da empresa **deve** ser registrado junto ao Departamento de TI. O registro implicará na aceitação dos termos desta política.

5.3.2 Requisitos Mínimos de Segurança do Dispositivo

Para ser elegível ao programa BYOD, o dispositivo pessoal **deve** atender aos seguintes requisitos mínimos de segurança:

- **Autenticação de Acesso:** O dispositivo deve ter uma senha de bloqueio, PIN, padrão de desbloqueio ou autenticação biométrica (impressão digital, reconhecimento facial) ativada.
- **Sistema Operacional:** O sistema operacional deve estar sempre atualizado com as últimas versões e patches de segurança fornecidos pelo fabricante.
- **Software de Segurança:** Dispositivos como laptops devem ter um software de antivírus/antimalware aprovado pela empresa e mantido atualizado.
- **Criptografia:** O armazenamento do dispositivo (disco rígido, memória interna) deve ser criptografado para proteger os dados em caso de perda ou roubo.
- **Não-Jailbreak/Root:** O dispositivo não pode ter passado por processos de jailbreak (iOS) ou root (Android), que removem importantes camadas de segurança do sistema operacional.

5.3.3 Acesso à Rede e aos Dados

- O acesso à rede corporativa a partir de dispositivos pessoais deve ser feito exclusivamente através de canais seguros, como a rede Wi-Fi para convidados (se aplicável e segregada) ou através de uma Conexão VPN (Virtual Private Network) fornecida pela empresa.
- O armazenamento de dados corporativos classificados como **Confidenciais** ou **Restritos** no armazenamento local de dispositivos pessoais é **estritamente proibido**, a menos que seja dentro de um contêiner seguro ou aplicação gerenciada pela empresa.
- A empresa poderá implementar soluções de Gerenciamento de Dispositivos Móveis (MDM - Mobile Device Management) ou Gerenciamento de Aplicações Móveis (MAM - Mobile Application Management) para criar um ambiente corporativo seguro e separado no dispositivo pessoal.

5.4 Responsabilidades do Usuário

O proprietário do dispositivo é responsável por:

- **Manutenção e Custos:** O colaborador/empresa é responsável pela aquisição, manutenção, seguro e custos de conexão (planos de dados) do dispositivo.
- **Segurança Física:** Proteger o dispositivo contra perda, roubo e acesso não autorizado.
- **Uso Aceitável:** Utilizar o dispositivo de forma ética e profissional, em conformidade com a Política de Segurança da Informação e outras políticas da empresa.
- **Backup de Dados Pessoais:** Realizar o backup de suas informações pessoais. A Allcance Soluções não se responsabiliza pela perda de dados pessoais (fotos, contatos, etc.) no dispositivo.
- **Notificação de Incidentes:** Em caso de perda, roubo ou comprometimento do dispositivo, o colaborador **deve notificar imediatamente** o Departamento de TI para que as medidas de segurança cabíveis (como a limpeza remota dos dados corporativos) possam ser tomadas.

5.5 Direitos da Allcance Soluções

A Allcance Soluções reserva-se o direito de:

- **Monitorar o Acesso:** Monitorar o acesso aos recursos corporativos a partir de dispositivos pessoais.
- **Auditar a Conformidade:** Verificar, a qualquer momento, se os dispositivos registrados estão em conformidade com os requisitos de segurança desta política.
- **Limpeza Remota (Remote Wipe):** Em caso de perda, roubo do dispositivo ou término do contrato de trabalho, a empresa tem o direito de remover remotamente **apenas os dados corporativos** do dispositivo. Dependendo da tecnologia utilizada (MDM/MAM), isso pode significar a remoção do perfil de trabalho ou, em casos extremos e como última opção, a redefinição do dispositivo para as

configurações de fábrica (o que apagaria também os dados pessoais). O colaborador, ao aderir ao BYOD, consente com este procedimento.

5.6 Privacidade

A Allcance Soluções respeita a privacidade de seus colaboradores. A empresa não monitorará o uso pessoal do dispositivo, como chamadas, mensagens de texto pessoais, e-mails pessoais ou histórico de navegação pessoal. O monitoramento e as capacidades de gerenciamento se restringem ao contêiner corporativo e ao acesso aos recursos da empresa.

5.7 Término do Acesso

O acesso aos dados e sistemas da empresa será revogado imediatamente após o término do vínculo empregatício. O colaborador concorda em cooperar com o Departamento de TI para garantir que todos os dados corporativos sejam removidos de seu dispositivo pessoal de forma segura.

5.8 Sanções

O não cumprimento desta política pode resultar em medidas disciplinares, incluindo a revogação do privilégio de uso de dispositivo pessoal, advertência, suspensão e, em casos graves, demissão por justa causa, além das sanções legais cabíveis.

6. Glossário de Termos

Termo	Definição
BIA	Business Impact Analysis (Análise de Impacto nos Negócios)
BYOD	Bring Your Own Device (Traga seu Próprio Dispositivo)
CISO	Chief Information Security Officer
ERIS	Equipe de Resposta a Incidentes de Segurança
LGPD	Lei Geral de Proteção de Dados Pessoais
MAM	Mobile Application Management (Gerenciamento de Aplicativos Móveis)
MDM	Mobile Device Management (Gerenciamento de Dispositivos Móveis)
PSI	Política de Segurança da Informação
RPO	Recovery Point Objective (Objetivo de Ponto de Recuperação)
RTO	Recovery Time Objective (Objetivo de Tempo de Recuperação)

allcance
SOLUÇÕES

NOSSA MISSÃO É PROPORCIONAR SOLUÇÕES TECNOLÓGICAS INOVADORAS E DE ALTA QUALIDADE, GARANTINDO CONECTIVIDADE, SEGURANÇA E EFICIÊNCIA.

HTTPS://WWW.ALLCANCESOLUCOES.NET.BR