Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria
Diretoria de Tecnologia da Informação

PROCESSO DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS SEGURANÇA DA INFORMAÇÃO EM SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
08/01/2024	1	Elaboração do processo de gestão de continuidade de negócios em segurança da informação em serviços de Tecnologia da Informação.

1. INTRODUÇÃO

Gestão de continuidade de negócios (GCN) é um processo estratégico que visa identificar ameaças potenciais para o IFTO e desenvolver planos e estratégias para garantir a continuidade das operações, minimizando impactos em caso de eventos adversos. Este processo envolve a análise de riscos, identificação de áreas críticas de negócios, desenvolvimento de planos de resposta a emergências e recuperação de desastres, além de garantir a resiliência operacional do IFTO.

A GCN é fundamental para ajudar as organizações a enfrentar interrupções inesperadas, como desastres naturais, crises cibernéticas, ou qualquer outro evento que possa afetar negativamente suas operações. O objetivo principal deste processo é garantir que a instituição possa continuar suas operações ou retomá-las rapidamente após enfrentar interrupções ou incidentes que possam ameaçar sua estabilidade e funcionamento normal.

Neste sentido, o processo de gestão de continuidade de negócios em segurança da informação em serviços de TI do IFTO é baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio. Este processo é composto por um plano de continuidade de negócios, o qual observará o disposto no relatório de identificação, análise e avaliação de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio (BRASIL, 2021).

Dentro do contexto apresentado, este documento apresenta uma breve introdução, definições, gestão de continuidade de negócios em

segurança da informação em serviços de TI, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências.

1.1. **Escopo**

O escopo do processo de gestão de continuidade de negócios em segurança da informação em serviços de TI é amplo e abrange desde a identificação de riscos e avaliação de impacto até o desenvolvimento de planos detalhados e a realização de testes para garantir a resiliência dos serviços de TI em situações adversas. Ele abrange:

a) análise de impacto nos negócios (BIA): Identificação e avaliação dos serviços de TI essenciais para o negócio. Isso envolve determinar quais sistemas, aplicativos e processos são críticos e sua interdependência;

b) identificação de riscos e ameaças: identificação de ameaças potenciais (como desastres naturais, falhas de sistema, ataques cibernéticos) que podem interromper os serviços de TI;

c) desenvolvimento de planos de continuidade de negócios: criação de planos detalhados para garantir a continuidade das operações de TI, incluindo procedimentos de *backup,* recuperação de desastres, realocação de recursos, entre outros;

d) testes e exercícios: realização de testes periódicos para garantir que os planos de continuidade de negócios estejam atualizados e sejam eficazes em situações reais;

e) gestão de crises e resposta a incidentes: definição de procedimentos claros para lidar com crises e incidentes de segurança de TI de maneira rápida e eficaz;

f) treinamento e conscientização: capacitação dos usuários para entenderem seus papéis e responsabilidades durante uma interrupção, além de conscientização sobre práticas de segurança; e

g) melhoria contínua: revisão constante dos processos e procedimentos para identificar áreas de melhoria e garantir a atualização contínua dos planos de continuidade.

1.2. **Objetivos**

O processo de gestão de continuidade de negócios em segurança da informação em serviços de TI tem como objetivo geral investigar, desenvolver e implementar opções de recuperação de serviços de TI, de forma que o IFTO esteja preparado para enfrentar e se recuperar de situações adversas, mantendo seus serviços de TI essenciais em funcionamento e protegendo seus ativos críticos. Para isso são definidos os seguintes objetivos específicos:

a) manter a continuidade operacional: garantir que os serviços de TI essenciais para o negócio continuem funcionando, mesmo após a ocorrência de eventos disruptivos, como falhas de sistemas, desastres

naturais ou ataques cibernéticos;

b) reduzir o tempo de inatividade: minimizar o tempo em que os serviços de TI ficam indisponíveis em situações de crise, através de planos de recuperação e estratégias de mitigação de riscos;

c) proteger os ativos de TI: garantir a integridade e segurança dos ativos de tecnologia da informação, incluindo dados, sistemas e infraestrutura, contra ameaças e danos;

d) cumprir requisitos regulatórios: assegurar que o IFTO esteja em conformidade com regulamentações e requisitos legais relacionados à continuidade de negócios e proteção de dados;

e) minimizar impactos financeiros: reduzir os impactos financeiros decorrentes de interrupções nos serviços de TI, como perda de receita, custos de recuperação e danos à reputação;

f) melhorar a resiliência: desenvolver e implementar estratégias que aumentem a resiliência dos sistemas de TI, permitindo uma rápida adaptação e recuperação em situações adversas;

g) estabelecer processos de resposta a incidentes: ter procedimentos claros para lidar com incidentes de segurança cibernética, desastres naturais, falhas de sistemas, entre outros, visando minimizar o impacto e acelerar a recuperação; e

h) conscientização e preparação: educar e treinar servidores para lidar com situações de emergência, garantindo que eles compreendam seus papéis e responsabilidades durante a continuidade de negócios.

1.3. **Abrangência**

A abrangência do processo de gestão de continuidade de negócios em segurança da informação de serviços de TI é holística, envolvendo não apenas a parte técnica dos sistemas de TI, mas também aspectos operacionais, de comunicação, gestão de riscos e recursos humanos para garantir a resiliência e a continuidade dos negócios em cenários adversos. Ele envolve:

a) análise de impacto nos negócios: avaliar o impacto que a interrupção desses ativos teria no negócio, considerando aspectos como tempo de inatividade tolerável, perda financeira e reputacional;

b) avaliação de riscos e ameaças: identificar ameaças potenciais que podem afetar a continuidade dos serviços de TI, incluindo falhas de hardware, ataques cibernéticos, desastres naturais, entre outros;

c) desenvolvimento de planos de continuidade de negócios: criar planos detalhados que descrevam como restaurar os serviços de TI essenciais em caso de interrupção, incluindo estratégias de backup, recuperação e realocação de recursos;

d) testes e exercícios: realizar testes periódicos para garantir a eficácia dos planos de continuidade, identificar lacunas e ajustar os processos conforme necessário;

e) gestão de crises e resposta a incidentes: estabelecer procedimentos claros para lidar com incidentes de segurança cibernética, desastres naturais ou outras situações de emergência que possam afetar os serviços de TI;

f) recuperação de desastres: implementar estratégias e tecnologias para recuperar rapidamente os sistemas de TI após um evento adverso, visando minimizar o tempo de inatividade;

g) comunicação e conscientização: desenvolver planos de comunicação para informar as partes interessadas internas e externas sobre interrupções e o progresso na recuperação dos serviços de TI;

h) treinamento e capacitação: educar os funcionários sobre procedimentos de continuidade de negócios e seu papel na mitigação de danos e na recuperação dos sistemas de TI; e

i) melhoria contínua: realizar análises pós-incidentes para identificar oportunidades de melhoria nos processos de GCN e nos planos de continuidade.

1.4. **Benefícios esperados**

A partir da implementação do processo de gestão de continuidade de negócios em segurança da informação em serviços de TI espera-se obter os seguintes benefícios:

a) maior resiliência: ao planejar e implementar estratégias de continuidade, o IFTO se torna mais resiliente a interrupções. Isso significa uma capacidade ampliada de lidar com incidentes e desastres, minimizando o impacto nas operações de TI;

b) redução do tempo de inatividade: planos de continuidade bem elaborados ajudam a minimizar o tempo em que os serviços de TI ficam indisponíveis após uma interrupção. Isso significa menos perda de produtividade e menor impacto nos negócios;

c) proteção dos ativos de TI e dados: a gestão de continuidade de negócios ajuda a proteger os ativos de TI, como dados sensíveis, sistemas críticos e infraestrutura, mitigando os riscos de perda ou corrupção durante situações adversas;

d) conformidade e mitigação de riscos: a implementação de estratégias de continuidade de negócios ajuda as organizações a atenderem requisitos regulatórios e a reduzir os riscos associados à não conformidade;

e) redução de custos: embora a implementação inicial possa ter custos associados, a redução do tempo de inatividade e a capacidade de lidar com incidentes de forma eficiente podem resultar em economia a longo prazo;

f) confiança do usuário e reputação: a capacidade de manter os serviços durante situações adversas pode aumentar a confiança dos usuários do IFTO, protegendo sua reputação;

g) preparação para emergências: uma estratégia sólida de gestão de continuidade de negócios prepara a equipe para lidar com emergências,

reduzindo o pânico e a confusão durante situações críticas;

h) melhoria na tomada de decisões: o processo de gestão de continuidade de negócios requer uma compreensão profunda das operações de TI e de como elas se alinham com os objetivos de negócios. Isso pode levar a uma melhor tomada de decisões estratégicas;

i) agilidade e flexibilidade: capacidade de se adaptar rapidamente a mudanças e desafios inesperados, garantindo a continuidade dos negócios, mesmo em cenários imprevisíveis; e

j) melhoria contínua: através da revisão constante dos planos, testes e análises pós-incidentes, o IFTO pode melhorar continuamente seus processos de gestão de continuidade de negócios, tornando-se mais robustas e preparadas para o futuro.

2. DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão utilizados os seguintes conceitos e definições:

a) acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

b) adminsitrador de rede: pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade;

c) ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

d) análise de impacto nos negócios: visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para qualificar e quantificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos;

e) análise de incidentes: consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;

f) análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

g) ativo: qualquer coisa que tenha valor para a organização;

h) ativo de rede: equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

i) ativos de informação: os meios de armazenamento, transmissão e

processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

j) ataque: ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não integro, ou indisponível;

k) atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

l) avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

m) backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

n) banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam de forma a criar algum sentido (informação) e dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

o) computação em nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços;

p) comunicação de dados: transmissão, emissão ou recepção de dados ou informações de qualquer natureza por meios confinados, por radiofrequência ou por qualquer outro processo eletrônico ou eletromagnético ou ótico;

q) contingência: recursos iguais que estejam disponíveis na falta do ambiente principal. São exemplos: servidores, computadores, *nobreak*, equipamentos de conectividade e outros;

r) continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

s) controles de segurança: medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de*hash*, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e*backups*, entre outros;

t) criptografia: arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de

decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

u) crise: Interrupção significativa nos negócios de uma organização que estimula uma cobertura extensiva pela mídia. O resultado da opinião pública pode afetar suas operações e ainda pode ter impactos políticos, legais e financeiros em seus negócios;

v) desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

w) disponibilidade: qualidade de tornar disponível para usuários, sempre que necessário e para qualquer finalidade, a informação gerada ou adquirida por um indivíduo ou organização. Uma informação disponível é a que dela necessitam, no momento em que necessitam;

x) equipe de trtamento e resposta a incidentes cibernéticos: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

y) evento: qualquer mudança de estado que tenha significância para o gerenciamento de um serviço de TI ou outro item de configuração. O termo também pode ser usado para significar um alerta ou notificação criada por qualquer serviço de TI, item de configuração ou uma ferramenta de monitoramento. Pode ser considerado um evento: link de internet com consumo próximo a contratado junto a operadora, disco rígido de um servidor cheio, alto consumo de memória RAM;

z) firewall: recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um a conjunto de redes, ou a partir dela. Podem ser implementados em*hardware*ou*software*, ou em ambos. Cada mensagem que entra ou sai da rede passa pelo*firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

a1) gestão de continuidade: Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

b1) gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

c1) gestão de segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e

táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

d1) incidente: interrupção não planejada (imprevista) de um serviço ou redução na qualidade de um serviço. Qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado. Qualquer acontecimento que ocorre com algum componente que tenha alguma ligação com um serviço já prestado pelo departamento de TI e que não faça parte do comportamento padrão de usabilidade causando assim a redução na qualidade do serviço de TI ou até mesmo a interrupção do serviço como um todo, como por exemplo: internet lenta, indisponibilidade para acessar uma pasta na rede, e-mail não enviando mensagens e impressora não funcionando;

e1) informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

f1) Interrupção: evento que seja previsto ou não (por exemplo, um blecaute ou terremoto), que cause um desvio negativo, imprevisto na entrega e execução de produtos ou serviços da organização, de acordo com seus objetivos;

g1) tempo de recuperação (RTO – recovery time objective): tempo necessário para a recuperação dos serviços de TI e atividades do negócio após a ocorrência de um evento;

h1) plano de continuidade de negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

i1) política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);

j1) ponto de recuperação (RPO – recovery point objective): estado em que os serviços de TI serão disponibilizados após a recuperação;

k1) redes de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

l1) requisição: quando tudo esta funcionando perfeitamente nos serviços de TI, porem o usuário precisa da mão de obra do departamento de tecnologia para a criação de um recurso ou desenvolvimento de uma nova ferramenta de trabalho. Exemplo de requisição: criação de um e-mail, mudança da instalação de um computador, desenvolvimento de um novo relatório no sistema;

m1) risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade;

n1) risco de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um

conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

o1) segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

p1) serviços de tecnologia da informação: provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação;

q1) sistemas de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações em forma integrada;

r1) tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

s1) usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF.

3. GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO EM SERVIÇOS DE TI

Gestão de continuidade de negócio envolve o gerenciamento da recuperação ou da continuidade das atividades no caso de uma interrupção de negócios e o gerenciamento do programa de continuidade por meio de treinamentos, testes e análises críticas, de forma a garantir que os planos de continuidade estejam sempre atualizados. Este processo complementa a estrutura de gestão de riscos de forma a reagir adequadamente às interrupções operacionais enquanto protege os ativos de TI e permite a melhoria da segurança da informação.

A implementação do processo de gestão de continuidade de negócios em segurança da informação em serviços de TI tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou da entidade nessa área, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres. O processo de gestão de continuidade de serviços de TI é baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio (BRASIL, 2021).

A gestão de continuidade de negócios em segurança da informação em serviços de TI refere-se ao conjunto de práticas, estratégias e processos utilizados para garantir que os serviços de TI atendam às necessidades e objetivos do negócio do IFTO. Este processo abrange várias áreas como por exemplo: alinhamento estratégico, gestão de portólio de serviços, governança de TI, gestão de riscos em TI,

gerenciamento de relacionamento com clientes, melhoria contínua de processos, medição de desempenho e indicadores-chave de desempenho, gestão financeira e orçamentária, gestão de projetos e mudanças e estratégias de inovação e tecnologia.

Segundo o *Information Technology Infrastructure Library* (ITIL) o processo de gestão de continuidade de negócios em segurança da informação em serviços de TI é destinado a dar suporte ao gerenciamento de continuidade de negócios, de forma a garantir que os serviços voltem a funcionar dentro dos prazos de negócios acordados após interrupções graves de serviço. O foco deste processo é o planejamento da prevenção de incidentes, previsão e gerenciamento, com o objetivo de manter a disponibilidade e o desempenho do serviço nos mais altos níveis antes, durante e depois de um incidente em nível de desastre (OGC, 2007).

Este processo garante que o provedor de serviço de TI tenha um nível mínimo de serviço acordado, através da redução do risco, a um nível aceitável em um evento de desastre. Ele envolve:

a) definir uma política de gestão de continuidade de negócios em segurança da informação em serviços de TI;

b) definir necessidade e requisitos mínimos para a estrutura de retorno, em caso de paradas de serviços de TI;

c) analisar riscos de desastres com os serviços de TI, de forma a reduzi-los ou transferi-los para um terceiro;

d) desenvolver um plano de continuidade de negócios em segurança da informação em serviços de TI conforme as necessidades da organização;

e) planejar estruturas de retorno;

f) planejar e conscientizar a organização para situações de gravidade; e

g) realizar testes, auditoria, controle e gestão de mudanças na estrutura de retorno.

A partir do contexto apresentado, processo de gestão de continuidade de negócios em segurança da informação em serviços de TI adotado pela área de TI do IFTO é apresentado na figura 1. Este processo é composto por 5 (cinco) fases baseadas no ciclo de melhoria contínua PDCA (Ciclo de Deming).

Figura 1 - Processo de gestão de continuidade de negócio

A figura 1 apresenta as fases do processo de gestão de continuidade de negócios em segurança da informação em serviços de TI. Estas fases envolvem atividades relacionadas com iniciação, requerimentos e estratégia, implementação, operação e invocação de um plano de gestão de continuidade de negócios em segurança da informação em serviços de TI. A tabela 1 apresenta o detalhamento deste processo.

Tabela 1 - Processo de gestão de continuidade de negócios em segurança da informação em serviços de TI

Processo de gestão de continuidade de negócios em segurança da informação em serviços de TI	
Entrada	Informações sobre os serviços e os níveis de serviço do gerenciamento de catálogo de Serviço e nível de serviço.
Fases	1. Planejamento e iniciação. 2. Análise de impacto nos negócios. 3. Estratégias de recuperação. 4. Desenvolvimento e implementação. 5. Manutenção e revisão.
Saída	Plano de gestão de continuidade de negócios em segurança da informação em serviços de TI.

3.1. **Planejamento e iniciação**

A fase de planejamento e iniciação em continuidade de negócios em segurança da informação em serviços de TI é crucial para garantir que o IFTO esteja preparado para enfrentar e se recuperar de eventos disruptivos. Esta fase é responsável pela definição de políticas, objetivos, metas, processos e procedimentos relevantes para a gestão de

continuidade de negócios em segurança da informação em serviços de TI. Ela envolve a execução das seguintes atividades:

a) entender a organização, reconhecendo a necessidade de continuidade de negócios em segurança da informação em serviços de TI;

b) definir o escopo da gestão de continuidade de negócios em segurança da informação em serviços de TI;

c) definir os termos de referência de gestão de continuidade de negócios em segurança da informação em serviços de TI;

d) definir as estratégias para a gestão de continuidade de negócios em segurança da informação em serviços de TI;

e) alocar recursos para a gestão de continuidade de negócios em segurança da informação em serviços de TI;

f) definir papéis e responsabilidades para a gestão de continuidade de negócios em segurança da informação em serviços de TI;

g) estabelecer políticas e objetivos; e

h) alocar recursos (humanos, tecnológicos e financeiros).

3.2. **Análise de impacto nos negócios**

A fase análise de impacto nos negócios visa avaliar o impacto potencial de interrupções nos processos e operações críticas do IFTO. A análise de impacto nos negócios fornece informações valiosas para orientar o desenvolvimento de estratégias de continuidade de negócios, permitindo que a instituição concentre seus recursos onde são mais necessários para manter as operações críticas em funcionamento durante e após uma interrupção.

Esta fase é fundamental para identificar prioridades, estabelecer metas realistas e desenvolver estratégias eficazes para a continuidade operacional. Ela envolve as seguintes atividades:

a) identificação e mapeamento dos processos de negócios que são essenciais para o funcionamento do IFTO;

b) classificação dos processos com base em sua importância para as operações globais;

c) análise das relações e dependências entre os diversos processos e sistemas;

d) identificação de recursos compartilhados e interdependências que podem afetar a continuidade operacional;

e) avaliação do impacto financeiro de interrupções nos processos críticos;

f) estabelecimento de metas de tempo para a recuperação de processos críticos;

g) definição de janelas de recuperação aceitáveis para minimizar perdas e interrupções;

h) identificação e alocação de recursos humanos, tecnológicos e físicos necessários para a continuidade operacional;

i) avaliação da disponibilidade e capacidade desses recursos;

j) identificação dos riscos residuais após a implementação de medidas de mitigação;

k) análise de lacunas entre as capacidades atuais e as necessárias para atender aos objetivos de continuidade;

l) classificação dos processos críticos e recursos em termos de prioridade para a continuidade;

m) fornecimento de informações essenciais para orientar o desenvolvimento de estratégias de recuperação;

n) registro de todas as descobertas e decisões durante a análise de impacto nos negócios;

o) criação de documentação que servirá como base para o desenvolvimento de planos de continuidade; e

o) revisão periódica da análise de impacto nos negócios para garantir que esteja alinhada com as mudanças no IFTO, nos processos ou no ambiente de negócios.

3.3. **Estratégias de recuperação**

A fase estratégias de recuperação é fundamental para desenvolver planos específicos que permitirão o IFTO recuperar suas operações essenciais após uma interrupção significativa. Essa fase visa identificar e implementar estratégias eficazes para restaurar as operações críticas de uma organização dentro das janelas de recuperação estabelecidas. Ela envolve as seguintes atividades:

a) desenvolvimento de estratégias para mitigar os impactos identificados;

b) estabelecimento de planos de recuperação de desastres e continuidade de negócios em segurança da informação em serviços de TI;

c) implementação de medidas preventivas e de contingência;

d) estabelecimento de sequências de ações, responsabilidades e recursos necessários para a recuperação;

e) estabelecimento de acordos e planos de ação conjuntos;

f) realização de testes regulares e exercícios para validar a eficácia das estratégias de recuperação;

g) identificação de áreas de melhoria e ajustes nos planos com base nos resultados dos testes;

h) desenvolvimento de procedimentos claros de comunicação para garantir uma resposta rápida e coordenada durante a implementação das estratégias de recuperação;

i) estabelecimento de canais de comunicação eficazes com partes interessadas internas e externas; e

j) treinamento regular da equipe responsável pela execução das estratégias de recuperação.

3.4. **Desenvolvimento e implementação**

Desenvolvimento e implantação é uma fase crítica para garantir a resiliência do IFTO em face de eventos imprevistos. Esta fase responsável por implementar os planos, agenda de testes e relatórios, controles, processos e procedimentos. Ela envolve as seguintes atividades:

a) elaboração do plano detalhado de continuidade de negócios em segurança da informação em serviços de TI;

b) treinamento de servidores e partes interessadas;

c) desenvolvimento estratégias para mitigar os riscos e garantir a continuidade das operações;

d) formação de uma equipe responsável pela implementação e manutenção do plano de continuidade de negócios;

e) documentação de procedimentos detalhados para a recuperação de sistemas, processos e comunicações;

f) estabelecimento de protocolos de comunicação para informar as partes interessadas internas e externas durante uma interrupção;

g) realização de testes regulares do plano para garantir eficácia e fazer ajustes necessários;

h) capacitação da equipe responsável pelo plano de continuidade de negócios em segurança da informação em serviços de TI;

i) implementação o plano de continuidade de negócios em uma escala menor para identificar possíveis problemas antes da implementação em todo o IFTO; e

J) expansão da implementação do plano de continuidade de negócios para todos os setores do IFTO, garantindo que todos estejam cientes e preparados para seguir os procedimentos.

3.5. **Manutenção e revisão**

Fase responsável por realizar a manutenção e a revisão do processo de continuidade de negócios, e quando aplicável medir o desempenho do processo em relação às políticas, objetivos e experiências práticas e reportar os resultados através de análise crítica. Esta fase é responsável por avaliar periodicamente o desempenho e a conformidade e promover os ajustes necessários. Ela envolve as seguintes atividades:

a) atualização contínua do plano de continuidade de negócios em segurança da informação em serviços de TI para refletir mudanças organizacionais, tecnológicas ou de risco;

b) revisão após incidentes reais para identificar melhorias;

c) garantia de conformidade com regulamentos e padrões vigentes;

d) manutenção e atualização contínua da documentação dos planos de recuperação para refletir mudanças na organização, processos ou ambiente de negócios; e

e) avaliação constante das estratégias de recuperação à medida que a

organização evolui, garantindo que estejam alinhadas com as mudanças nas operações e no ambiente de negócios.

4. **PAPÉIS E RESPONSABILIDADES**

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Os papéis e responsabilidades definidos no processo de gerenciamento de continuidade de serviços de TI são:

4.1. **Alta Administração**

Este papel representa o mais alto nível estratégico e decisório do IFTO, seja ela parte da administração pública federal. Compete ao representante deste nível as seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de continuidade de negócios, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

b) disponibilizar os recursos (humanos, tecnológicos e financeiros) para a execução da política, norma interna complementar e processo de continuidade de negócios no âmbito do IFTO.

4.2. **Comitê Gestor de Tecnologia da Informação**

Representado por Pró-Reitorias, Diretorias Sistêmicas e Direção de Geral de Campus. É responsável pela decisão final sobre o escopo, política e diretrizes sobre a gestão de continuidade de negócios. Este papel tem as seguintes responsabilidades:

a) aprovar a estratégia de continuidade de negócios em segurança da informação em serviços de TI;

b) aprovar as diretrizes estratégicas que norteiam a elaboração do plano de gestão de continuidade de negócios em segurança da informação em serviços de TI;

c) disponibilizar os recursos necessários (humanos, tecnológicos e financeiros) para estabelecer, implementar, operar e manter o plano de gestão de continuidade de negócios em segurança da informação em serviços de TI.

4.3. **Comitê de Segurança da Informação**

Este grupo de pessoas representam áreas finalísticas do IFTO. Compete a este grupo de pessoas a seguinte responsabilidade:

a) avaliar e aprovar a política, norma interna complementar e processo

de gestão de continuidade de negócios em segurança da informação em serviços de TI.

4.4. **Gestor de Segurança da Informação**

Servidor(a) designado para gerir a segurança da informação. Compete à esta pessoa as seguintes responsabilidades:

a) elaborar e coordenar o processo de gestão de continuidade de negócios em segurança da informação em serviços de TI conjuntamente com a área de TI, considerando os aspectos de segurança da informação;

b) realizar ajustes no processo de gestão de continuidade de negócio em relação à segurança da informação com a finalidade de estar em conformidade com a legislação vigente no âmbito da administração pública federal; e

c) designar um agente responsável pela execução das atividades referentes ao processo de gestão de continuidade de serviços de TI, dentre os servidores efetivos do IFTO.

4.5. **Equipe de Tratamento e Resposta de Incidentes Cibernéticos**

Equipe responsável pela gestão do processo de continuidade de serviços de TI, representada por assistentes, técnicos, e analistas lotados na área de TI e Infraestrutura. Compete à estas pessoas a seguinte responsabilidade:

a) avaliar a política, norma interna complementar, processo, plano, procedimentos e atividades sobre gestão de continuidade de negócios em segurança da informação em serviços de TI.

4.6. **Setor de TI (Diretoria de Tecnologia da Informação e demais Setores de TI das unidades do IFTO)**

Agente responsável pela execução das atividades referentes ao processo de gestão de continuidade de serviços de TI. Representado pelo responsável pela área de TI no IFTO. Este papel tem as seguintes responsabilidades:

a) assessorar os responsáveis pelo processo ou os titulares das unidades em que forem identificadas atividades críticas nas atribuições referentes a gestão de continuidade de serviços de TI;

b) avaliar o plano de continuidade de negócios em segurança da informação em serviços de TI e propor mudanças, quando aplicável;

c) supervisionar a implementação, os testes de funcionamento e a atualização do plano de continuidade de negócios em segurança da informação em serviços de TI;

d) propor melhorias na implementação de novos controles relativos ao

plano de continuidade de negócios em segurança da informação em serviços de TI;

e) participar da elaboração da análise de impacto nos negócios; e

f) propor medidas visando ao desenvolvimento da cultura de gestão de continuidade de negócios em segurança da informação em serviços de TI.

4.7. **Coordenação de Redes e Segurança da Informação**

Setor responsável pelo processo em que forem identificadas atividades críticas. Compete à este setor as seguintes responsabilidades:

a) propor as diretrizes a serem contempladas no plano de continuidade de negócios em serviços de TI com base em processos de segurança da informação;

b) elaborar o plano de continuidade de negócios em segurança da informação em serviços de TI;

c) realizar os testes de funcionamento do plano de continuidade de negócios em segurança da informação em serviços de TI com base em requisitos de segurança da informação;

d) avaliar e aprimorar o plano de continuidade de negócios em segurança da informação em serviços de TI a partir dos resultados dos testes de funcionamento;

e) gerenciar a contingência quando ocorrer a interrupção de atividades, com base no plano de continuidade de negócios em segurança da informação em serviços de TI desenvolvido; e

f) propor os recursos necessários para a implementação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes de funcionamento do plano de continuidade de negócios em segurança da inforomação em serviços de TI.

4.8. **Usuários**

Pessoas que utilizam os dados e informações processados pelo IFTO. Cabe aos usuários as seguintes responsabilidades:

a) utilizar os dados e informações no IFTO prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;

b) notificar incidentes de segurança da informação; e

c) evitar na medida do possível se envolver em incidentes de segurança da informação.

5. **MATRIZ RACI**

A matriz RACI apresentada na tabela 2 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: ***responsible, accountable, consulted e informed***.

a) ***responsible (responsável):*** pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

b) ***accountable (responsabilizado):*** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um accountable;

c) ***consulted (consultado):*** pessoa que deverá ser consultada durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade;

d) ***informed (informado):*** pessoa que será informada acerca do progresso da execução da atividade.

Tabela 2 - Matriz de responsabilidades

Fase	AA	CGTI	CSI	GSI	ETIR	STI	CRSI	U
Planejamento e iniciação	A	C	C	C	C	C	R	I
Análise de impacto nos negócios	A	C	C	C	C	C	R	I
Estratégias de Recuperação	A	C	C	C	C	C	R	I
Desenvolvimento e implementação	A	C	C	C	C	C	R	I
Manutenção e revisão	A	C	C	C	C	C	R	I

Legenda:

AA: Alta Administração.

CGTI: Comitê Gestor de Tecnologia da Informação.

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

STI: (Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO).

CRSI: Coordenação de Redes e Segurança da Informação.

U: Usuários.

6. INDICADOR DE DESEMPENHO

O processo de gestão de continuidade de negócios em segurança da informação em serviços de TI será monitorado e avaliado periodicamente através de indicador de desempenho de forma a realizar

eventuais ajustes necessários. Este monitoramento tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. Para medir a eficiência deste processo foi definida a métrica operacional detalhada na tabela 3.

Tabela 3 - Indicador de desempenho

Indicador	Quantidade de serviços de TI contemplados no plano de continuidade de negócio em segurança da informação em serviços de TI.
Descrição	Número de serviços de TI contemplados no plano de continuidade de negócios em segurança da informação em serviços de TI.
Objetivo	Aumentar o número de serviços de TI contemplados no plano de continuidade de negócios em segurança da informação em serviços de TI.
Periodicidade	Anual
Fonte	Diretoria de Tecnologia da Informação
Fórmula	Somatório de serviços contemplados no plano de continuidade de negócios em segurança da informação em serviços de TI.
Meta	Aumentar a quantidade de serviços de TI contemplados no plano de continuidade de negócios em segurança da informação em serviços de TI.

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, o processo de gestão de continuidade de negócios em segurança da informação em serviços de TI está interligado à outros processos que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO). A figura 2 apresenta estes processos.

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

As práticas recomendadas para o processo de gestão de continuidade de negócios em segurança da informação em serviços de TI são fundamentais para garantir a resiliência das operações em situações de crise ou emergência. Dentre as boas práticas recomendadas no mercado tem-se:

1. Análise de impacto nos negócios específica para TI: Identificar os sistemas, aplicativos e processos de TI críticos para o negócio e avaliar seu impacto em caso de interrupção.

2. Gestão de riscos de TI: avaliar os riscos exclusivos de TI, como vulnerabilidades de segurança cibernética, falhas de *hardware/software* e dependência de fornecedores, e crie estratégias para mitigá-los.

3. Planos de recuperação e continuidade de TI: desenvolver planos detalhados de recuperação de desastres específicos para sistemas de TI críticos, com procedimentos claros para restauração e continuidade.

4. Backup e restauração de dados: implementar e testar regularmente sistemas robustos de backup e recuperação de dados para garantir a integridade e disponibilidade das informações essenciais.

5. Gestão de capacidade e redundância: mantera sistemas de TI com capacidade suficiente para lidar com aumentos repentinos de demanda e estabeleça redundância em infraestrutura crítica para evitar pontos únicos de falha.

6. Testes e simulações de recuperação de TI: realizar simulações de

recuperação de desastres específicas de TI para garantir a eficácia dos planos e identificar áreas de melhoria.

7. Gestão de mudanças e versionamento: implementar procedimentos rigorosos para gerenciamento de mudanças em sistemas de TI, garantindo que atualizações não causem interrupções não planejadas.

8. Monitoramento e alertas proativos: estabelecer sistemas de monitoramento contínuo para detectar problemas de TI e implemente alertas proativos para identificar potenciais falhas antes que causem interrupções.

9. Treinamento e conscientização de TI: educar os usuários sobre os procedimentos de recuperação de TI e seus papéis durante uma crise, promovendo uma cultura de responsabilidade e preparação.

10. Revisão e atualização contínua: revisar regularmente os planos de continuidade de TI, ajustando-os de acordo com mudanças nos sistemas, na infraestrutura ou nos requisitos do negócio.

11. Gestão de crises e resposta a incidentes: estabelecer uma equipe de resposta a incidentes bem treinada e prepare protocolos para lidar com diferentes tipos de emergências.

11. Comunicação: desenvolver planos de comunicação para manter as partes interessadas informadas durante uma crise.

12. Gerenciamento de fornecedores e parceiros: garantir que fornecedores e parceiros também tenham planos de continuidade e se alinhem aos requisitos da sua organização.

13. Liderança e comprometimento: ter o comprometimento da liderança da organização para a implementação e manutenção dos processos de gestão de continuidade de serviços de TI.

9. **REFERÊNCIAS**

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 3, de 28 de maio de 2021.** Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. Disponível em: https://www.in.gov.br/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172 Acesso em: 4 de jan. 2024.

Office of Government Commerce (OGC). ***ITIL v3 Service Strategies.*** Inglaterra: TSO 2007. Vol1.

Office of Government Commerce (OGC). ***ITIL v3 Service Design.*** Inglaterra: TSO 2007. Vol2.

Office of Government Commerce (OGC). ***ITIL v3 Service Transition.*** Inglaterra: TSO 2007. Vol3.

Office of Government Commerce (OGC). ***ITIL v3 Service Operation.*** Inglaterra: TSO 2007. Vol4.

Office of Government Commerce (OGC). **ITIL v3 Service Continual Service Improvement.** Inglaterra: TSO 2007. Vol5.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 08/01/2024, às 10:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2218370** e o código CRC **F1518040**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.000381/2021-10 SEI nº 2218370