Plano de Contingência da Informação
CONDGO
25/11/2025
OBJETIVO
Uma vez que falhas nos serviços de TI impactam diretamente nos setores administrativos da CONDGO, almeja-se com este plano prover medidas de proteções rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais. Este plano também objetiva estabelecer procedimentos de comunicação e mobilização para controle, em caso de contingências e emergências que possam ocorrer durante as atividades relacionadas a Tecnologia da Informação, visando aplicar as ações necessárias para correção e /ou eliminação do problema
APLICAÇÃO
Este documento se aplica a todos os serviços de tecnologia da informação que são executados na CONDGO.
DEFINIÇÕES
Acionamento: É o processo de comunicação com as equipes envolvidas no controle da emergência, de acordo com a ordem estabelecida para que as equipes desempenhem as atividades sob sua responsabilidade, a fim de controlar a emergência.
Administrador do plano de Contingência: Responsável pela manutenção e atualização dos dados e procedimentos necessários à plena operacionalidade do Plano de Contingência.
Áreas Sensíveis: Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência.
Áreas Vulneráveis: Áreas atingidas pela extensão dos efeitos provocados por um evento de falha.
Contingência: Situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos e que, ocorrendo, se transformará em uma situação de emergência. Diz respeito a uma eventualidade, possiblidade de ocorrer
Disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;
Incidente: É o evento não programado, de grande proporção, capaz de causar danos graves aos sistemas e aos equipamentos da TI.
Hipótese Acidental: Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e/ou equipamentos de TI.
Intervenção: É a atividade de atuar durante a emergência, seguindo ações planejadas, visando minimizar os possíveis dados aos equipamentos e sistemas de TI.
Situação de Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos que resulte ou possa resultar em danos próprios sistemas ou equipamentos ou ao desempenho do trabalho dos colaboradores da CONDGO.
Política de Segurança em Tecnologia da Informação: É um conjunto de documentos que descrevem quais são os objetivos que todas as atividades ligadas à segurança da informação na empresa devam ser alcançadas.
REFERÊNCIAS
Norma Técnica ABNT NBR ISO/IEC 27002:2022, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
Norma ABNT NBR ISO/IEC 27001:2022, Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos.
RESPONSABILIDADES
5.1 Diretoria Executiva
Aprovar o conteúdo desta norma, seus documentos associados e respectivas alterações, bem como propiciar os meios e recursos orçamentários necessários para a Gestão da Segurança da Informação.
Coordenar, orientar e avaliar as atividades relativas à segurança da informação na empresa.
5.2 Comitê de Segurança da Informação
Coordenar, orientar as atividades relativas à segurança da informação na empresa.
Submeter esta norma e demais documentos para aprovação da Diretoria Executiva.
Revisar e alterar esta norma, sempre que se fizer necessário.
Auxiliar na elaboração das normas e procedimentos associados a esta norma.
Monitorar a aplicação das diretrizes desta norma.

Gerenciar a implementação de controles necessários para aplicação destas diretrizes.

5.3 Colaboradores

Obedecer às diretrizes desta norma, mantendo a constante vigilância sobre as informações custodiadas ou de propriedade da empresa.

Informar aos membros do Comitê de Segurança da Informação qualquer necessidade de alteração nesta norma.

DESCRIÇÃO DAS ATIVIDADES

Responsabilidade

A equipe de Segurança da Informação deve fornecer suporte técnico, auxiliando os colaboradores da CONDGO em todo trabalho computacional ou que envolva indiretamente os sistemas corporativos e equipamentos da organização. Sua responsabilidade também consiste em administrar o local físico e informar a um nível superior sobre os problemas identificados para solução de forma rápida e precisa.

Níveis de Incidente

Nível I – Hipótese acidental que pode ser controlada pela equipe de TI e que não afeta o andamento do trabalho da organização. Ex: Problemas com equipamentos periféricos de computadores.

Nível II – Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo colaborador. Ex: Problema com o funcionamento do computador (não liga, travando etc.) ou ainda sistema offline impedindo o uso do mesmo.

Nível III – Hipótese acidental que impede o uso de sistemas ou equipamentos de toda a organização, impedindo assim o desenvolvimento do trabalho de todos os colaboradores. Ex: Falha na conexão com a internet ou queda de energia elétrica ou ainda problema técnico em algum servidor de rede que controla a conexão interna.

Nível IV – Hipótese acidental que impede o uso de sistemas para internamente e externamente, afetando não só a equipe interna como seus respectivos clientes.

Nível V - Hipótese acidental que impede o uso de sistemas para toda a empresa. Todo o trabalho da organização é suspenso ou impedido pela falha. Ex. Servidores e dados foram comprometidos através de um vírus ou ataque.

Principais riscos

Problemas, Incidentes e Devidas Ações de Contingência:

Para qualquer outro tipo de problema que envolva a TI, como problemas com equipamentos, problemas com configurações de e-mail, impressoras, problemas de acesso que envolva login e senha e etc. Os passos a serem seguidos são os seguintes:

Informar o problema Setor suporte de TI enviando um e-mail para o endereço seguranca@condgo.com.br

O chamado de suporte chega até o suporte de TI e o atendimento é agendado.

Caso seja necessário, o chamado será escalonado para outros setores ou responsáveis. - Após o atendimento o solicitante é informado da conclusão/resolução do problema reclamado

Comunicação

Quem deve comunicar

Qualquer colaborador que detecte qualquer tipo de problema que diga respeito a sistemas, equipamentos e/ou infraestrutura de TI

A quem comunicar

A comunicação deve ser feita para o Setor de Suporte de TI da CONDGO

Como comunicar

Os problemas detectados devem ser informados através do e-mail para o endereço seguranca@condgo.com.br

DISPOSIÇÕES GERAIS

Toda e qualquer excepcionalidade ou caso omisso nesta norma deve ser analisado pelo Comitê de Segurança da Informação.

Esta norma deve ser reavaliada no prazo máximo de 01 (um) ano, a partir da data de sua aprovação, ou sempre que se fizer necessário, a fim de garantir a manutenção das diretrizes de segurança da informação, quanto à sua atualização, aprovação e divulgação.

O não cumprimento dos termos desta norma sujeita o contratado, prestadores de serviços, parceiros e fornecedores infrator às penalidades previstas nas legislações cabíveis.

REGISTROS

Não se aplica.

ANEXOS

Não se aplica.