Política de Controle de Acesso Lógico

Apresentação

Este documento e seus anexos definem as normas a serem seguidas no CONDGO relativas ao acesso lógico, aos ativos e aos sistemas de informação, de modo a possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas e armazenadas no servidor do CONDGO, sejam de caráter público ou privativo.

A elaboração e a atualização deste documento e de seus anexos são de responsabilidade da Comissão Local de Segurança da Informação, criada pela CSI – Comitê de Segurança da Informação do CONDGO.

Este documento é composto de uma parte principal e de seus anexos. O documento principal contém as definições e regras gerais. Os anexos são as definições e regras para temas, ou áreas específicas.

Escopo

Este documento define as regras e procedimentos gerais para o acesso lógico aos sistemas e ativos de informação, as regras específicas, de acordo com o tema, estarão declaradas nos anexos deste documento, os quais abordarão os seguintes pontos:

acesso à rede local;

acesso à rede sem fio

utilização de mensageria corporativa e instantânea;

acesso à internet e à intranet;

Público-Alvo

As regras aqui dispostas aplicam-se a todos colaboradores da CONDGO e a qualquer pessoa que interaja com a rede do CONDGO ou utilize os serviços de TI nela disponíveis.

Conceituação

Recursos de TI – Todo equipamento ou dispositivo que utilize tecnologia da informação, bem como qualquer recurso ou informação que seja acessível através desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local, internet, vpn, pendrives, smartcards, tokens, smartphones, modems sem fio, desktops, pastas compartilhadas na rede, etc.

CSI – Comitê de Segurança da Informação da CONDGO, com atribuições específicas, definidas na Política de Segurança da Informação

Sistema de Informação – Aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, que visa otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando- os em informação.

Credenciais de Acesso – Conjunto composto pelo nome de conta e respectiva senha, utilizada para ingresso ou acesso (login) em equipamentos, rede ou sistema.

Rede Local – Conjunto de recursos compartilhados através dos servidores de rede, switches e computadores clientes, onde circulam as informações corporativas.

Rede sem Fio – Sistema que interliga equipamentos através de ondas eletromagnéticas.

Ponto de Acesso sem Fio - Equipamento que compõe uma rede sem fio, concentrando as conexões de um ou mais equipamentos.

Sistemas de Mensageria – Sistemas que permitem o envio e a recepção de mensagens de correio eletrônico ou de mensagens instantâneas entre usuários, dentro e fora de uma instituição.

Objetivos

Definir regras claras e objetivas para o acesso lógico a informações, serviços e recursos de TI dentro da CONDGO.

Documentos de Referência

Norma Técnica ABNT NBR ISO/IEC 27002:2022, Tecnologia da informação

Técnicas de segurança – Código de prática para a gestão da segurança da informação.

Responsabilidades:

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.

Comitê de Segurança da Informação

7.2.1 Coordenar, orientar as atividades relativas à segurança da informação na empresa.

7.2.2- Submeter esta norma e demais documentos para aprovação da Diretoria Executiva.
7.2.3 Revisar e alterar esta norma, sempre que se fizer necessário.
7.2.3 Auxiliar na elaboração das normas e procedimentos associados a esta norma.
7.2.4 Monitorar a aplicação das diretrizes desta norma.
7.2.5 Gerenciar a implementação de controles necessários para aplicação destas diretrizes.
7.3 Colaboradores
7.3.1 Obedecer às diretrizes desta norma, mantendo a constante vigilância sobre as informações custodiadas ou de propriedade da empresa.
7.3.2 Informar aos membros do Comitê de Segurança da Informação qualquer necessidade de alteração nesta norma.
Anexo I
Acesso à Rede Local
Apresentação
Este documento faz parte da Política de Controle de Acesso Lógico. Os técnicos da área de suporte deverão tê-lo à disposição, citá-lo e disponibilizá-lo para os usuários sempre que forem questionados com relação aos procedimentos adotados para a criação de contas.
Objetivos
Definir as regras a serem seguidas relativas à criação de contas para acesso à rede da CONDGO.
Disposições Gerais
A criação de novas contas de acesso à rede se dará da seguinte forma:
Para colaboradores, após a abertura de chamado pelo setor de cadastro de pessoal da unidade de recursos humanos, informando o nome completo, lotação e matrícula do servidor.
Para estagiários – após a abertura de chamado pelo setor de cadastro de pessoal da unidade de recursos humanos, informando o nome completo, unidade de atuação, matrícula do estagiário e vigência do contrato.
Para prestadores de serviço – após a abertura de chamado pelo gestor do contrato, informando o nome completo, unidade de atuação, número e vigência do contrato, nome da empresa contratada e matrícula na empresa contratada (ou outro documento legalmente válido).
Nas substituições eventuais, caberá ao responsável informar o período para a configuração adequada da conta de acesso do prestador de serviço.
As contas de estagiários e prestadores de serviço serão configuradas para expiração automática concomitante à vigência do contrato.
Caberá ao titular da unidade solicitar ao Suporte Técnico a liberação ou restrição de privilégios de acesso aos documentos de sua unidade.
O gestor do contrato, ou responsável pela fiscalização dos serviços desempenhados pelo prestador de serviço, ficará responsável por recolher sua assinatura no Termo de Responsabilidade.
O solicitante de acesso para servidor ou estagiário deverá recolher sua assinatura no Termo de Responsabilidade.
É responsabilidade do RH solicitar ao Suporte Técnico o cancelamento da conta de acesso quando do desligamento ou afastamento do prestador de serviço.
O setor de cadastro de pessoal da unidade de recursos humanos deverá informar, o desligamento e a movimentação de lotação de servidores e de estagiários para as providências de bloqueio e posterior eliminação da conta, se for o caso.
Não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede.
Após a criação das contas de acesso do usuário, senhas de acesso devem ser escolhidas, conforme as seguintes exigências:
Toda senha deve possuir no mínimo 8 caracteres.
As senhas devem ser compostas como se segue:
A senha deve ter no mínimo 8 (oito) caracteres.
A senha deve conter caracteres provenientes de três das quatro categorias relacionadas abaixo:
Caracteres maiúsculos (A até Z).
Caracteres minúsculos (a até z).
Dígitos numéricos (0 a 9).
Caracteres não alfabéticos (por exemplo, !, $, #, %)
A senha deve ser obrigatoriamente alterada pelo usuário, quando da realização do primeiro acesso.

A senha será expirada a cada 120 (cento e vinte) dias. A nova senha deve ser diferente das 3 (três) últimas senhas.
A senha só pode ser alterada pelo usuário uma vez a cada 3 (três) dias.
A senha não poderá conter a data de nascimento, o nome do usuário ou uma sequência de três ou mais caracteres consecutivos que estejam presentes em seu nome completo.
A senha não deve conter partes do login ou nome do usuário que excedam 2 caracteres consecutivos.
Disposições Finais
As novas contas de acesso à rede serão compostas por nome e sobrenome do colaborador, sendo a forma padrão para login o nome e o último sobrenome, separados por ponto.
Caso a forma padrão encontre homônimos com conta já existente, será escolhida uma forma alternativa.
No ato de criação de conta de acesso à rede, será automaticamente criada conta dos serviços de mensageria instantânea, correio eletrônico e agenda correspondente, bem como de outros serviços que utilizem a mesma base de dados de autenticação.
Após a criação da conta solicitada, o Suporte Técnico deverá informar ao solicitante a criação da conta e a senha de acesso inicial juntamente com as instruções para a sua alteração.
Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.
Anexo II
Utilização do Sistema de Rede sem Fio
Apresentação
Este documento faz parte da Política de Controle de Acesso Lógico da CONDGO. A equipe de suporte técnico deve tê-lo à disposição, citá-lo e disponibilizá-lo para os usuários sempre que forem questionados com relação aos procedimentos adotados para o acesso e a utilização do serviço de rede sem fio.
Objetivos
Definir as regras a serem seguidas no âmbito da CONDGO.
Disposições Gerais
As exigências a seguir descritas atingem todos os dispositivos de comunicação de dados sem fio, como notebooks, smartphones e microcomputadores, conectados à rede corporativa da CONDGO.
Os pontos de acesso sem fio conectados à rede local da CONDGO, deverão ser registrados e aprovados pela diretoria da CONDGO. Esses pontos serão objeto de testes periódicos de penetração e de auditoria.
As conexões à rede sem fio poderão ser avaliadas pelo CSI e Suporte Técnico em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.
Os dispositivos conectados à rede da CONDGO através de conexão sem fio deverão utilizar as configurações de criptografia estabelecidas pelo Suporte Técnico.
Disposições Finais
Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.
Anexo III
Utilização de Sistemas de Mensageria
Apresentação
Este documento faz parte da Política de Controle de Acesso Lógico do CONDGO. Os técnicos do Suporte Técnico deverão tê-lo à disposição, citá-lo e disponibilizá-lo para os usuários sempre que forem questionados com relação aos procedimentos adotados para o acesso e a utilização de serviços de mensageria.
Objetivos
Definir as regras a serem seguidas pelo CONDGO relativas à utilização dos serviços de mensageria.
Disposições Gerais
O sistema de correio eletrônico do CONDGO não deve ser utilizado para a criação ou a distribuição de quaisquer mensagens que não sejam compatíveis com as atribuições dos usuários, incluindo as que contenham ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade, entre outros não relacionados à atividade do órgão.

Todos os e-mails armazenados no sistema de correio eletrônico do CONDGO e aqueles transmitidos ou recebidos por meio dele são passíveis de auditoria, podendo ser rastreados por softwares específicos para verificação e adequação às normas estabelecidas na Política de Segurança da Informação.
O envio de mensagens a todos os componentes da lista de endereços do CONDGO restringir-se-á a assuntos de interesse geral da empresa.
É proibido o envio de spam ou mensagens que contenham qualquer tipo de software malicioso pelos usuários do sistema de correio eletrônico da CONDGO.
O Suporte Técnico proverá mecanismos para a identificação de mensagens que possuam conteúdo infectado por softwares maliciosos ou que ofereçam risco à segurança da informação. Tais mensagens, quando detectadas, poderão ser excluídas automaticamente ou armazenadas em quarentena.
O usuário poderá enviar mensagens somente a 40 usuários por vez. Caso seja necessário maior quantidade deverá ser solicitado formalmente, com justificativa, ao Suporte Técnico. O tamanho do email também será restringido a 10MB, caso necessário, deverá ser solicitado formalmente, com justificativa, ao Suporte técnico.
Disposições Finais
Após a criação da conta solicitada, Suporte Técnico deverá informar ao solicitante e ao titular da conta a senha de acesso inicial juntamente com as instruções para sua alteração, quando aplicável.
Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.
No caso acima, os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis tanto o titular das credenciais quanto aquele que as utilizar indevidamente.
Anexo IV
Utilização de Internet e Intranet
Uso da Internet
Será concedido a todos os usuários da rede CONDGO o acesso à Internet através do perfil de Internet Básico. Cabe ao Responsável do usuário avaliar a necessidade de outros serviços e comunicar à TI.
Em casos de mudanças nas atribuições ou lotação do usuário, a readequação dos direitos de acesso à internet deve ser realizada mediante solicitação formal por parte do responsável pelo usuário.
O acesso à Internet é uma concessão temporária, revogável a qualquer tempo, nos termos da Política de Segurança da Informação da empresa;
Os acessos a internet são definidos por perfil: **Sites Específicos serão listados por cada área, e fornecidos em listagem em anexo, podendo ser alterados a qualquer momento de acordo com a necessidade.
Nas instalações da empresa todo acesso à Internet, através dos links corporativos, deve ser realizado por meio de conexões disponibilizadas e/ou autorizadas. Qualquer acesso não autorizado será detectado estando o mesmo sujeito à aplicação das penalidades cabíveis pelo uso indevido do recurso ou por danos causados à empresa.
Quando o usuário utilizar o acesso à Internet para a realização de transações que envolvam informações confidenciais da empresa deve adotar as seguintes regras de segurança:
Digitar o endereço do site diretamente no browser (navegador da Internet);
Não clicar em links indicados nas páginas de Internet ou mensagens de correio eletrônico de origem duvidosa;
Ao acessar sites de instituições financeiras, verificar a existência do uso de certificado digital e a validade do mesmo (cadeado indicativo na janela do navegador);
Quando da transmissão de informações, verificar se o endereço do site (URL) inicia-se por “HTTPS”;
Todo acesso efetuado a recursos da internet é monitorado e de responsabilidade do usuário, estando o mesmo sujeito à aplicação das penalidades cabíveis pelo uso indevido do recurso ou por danos causados à empresa.
O acesso à Internet da empresa não deve ser utilizado para:

Acessar sites de pornografia, pedofilia, hacking, atividades ilícitas, não-éticas, preconceituosas ou que façam incitação à violência e outros contrários à legislação e regulamentação em vigor, proxies anonimizadores, sites que possam ser utilizados para envio de spam ou phishing, compartilhamento de arquivos HTTP ou P2P, sites relacionados à jogos eletrônicos ou jogos de azar e sites relacionados à armas de fogo, mesmo que alguns desses sites não estejam bloqueados pelos mecanismos de segurança implementados, exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho realizadas.
Acessar sites com materiais atentatórios à moral e aos bons costumes, ofensivos ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares.
Executar atividades relacionadas a jogos eletrônicos.
Acessar conteúdo multimídia, exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho realizados na empresa.
Caso o colaborador necessite de algum acesso extra além daquele que foi disponibilizado a ele, deverá informar ao seu gestor direto, e providenciará o acesso necessário permanente, se for o caso, ou temporário sob monitoramento.
Anexo VI
Termo de Responsabilidade