**PLANO DE CONTROLE DE ACESSO À INFORMAÇÃO**

Data: 28/10/2021

Versão 2.0

**HISTÓRICO DE ALTERAÇÕES**

| **DOCUMENTO** |
| --- |
| **Descrição** | Documentação dos planos de Segurança da Informação |
| **Objetivo** | Este documento descreve os processos do Plano de Controle de Acesso à Informação. |
| **Responsável** | **Equipe** | **Criado em** |
| GESIN – DITI | 06/07/2021 |
| **Setor** | Gerência de Infraestrutura e Segurança da Informação - GESIN |

**SUMÁRIO**

[​ PLANO DE CONTROLE DE ACESSO À INFORMAÇÃO](#_heading=h.30j0zll) 4

[​](#_heading=h.1fob9te) IDENTIFICAÇÃO [DE USUÁRIOS](#_heading=h.tyjcwt) 5

[​ Registro de usuários de serviços de TI](#_heading=h.3dy6vkm) 5

[​ Provimento de acesso aos usuários](#_heading=h.86dnax8y1y6o) 5

[​ Gerenciamento de credencial de acesso](#_heading=h.rq1pqt64rrgk) 6

[​ CONTROLE DE ACESSO LÓGICO](#_heading=h.i13l0p959y15) 7

[​ Controle de acesso à rede de dados](#_heading=h.r60v0pk8du7c) 7

[​ Controle de acesso à rede sem fio](#_heading=h.do355jdpqlw2) 8

[​ Controle de acesso remoto](#_heading=h.kx7qdeneu3t7) 8

 [Controle de acesso aos arquivos e diretórios](#_heading=h.lwwpbm521yl3) 9

 Utilização de e-mail 9

 [CONTROLE DE ACESSO FÍSICO 1](#_heading=h.3hcgh2vhroms)0

 Perímetro externo 11

 Perímetro interno 11

 Acesso de visitantes 11

 Controle de chaves e alarmes 12

[​ AUDITORIA INTERNA 12](#_heading=h.qwcf9dud6ftk)

[​ Análise de perfis e direito de acesso aos usuários 13](#_heading=h.1p2vgt8ah29o)

**PLANO DE CONTROLE DE ACESSO À INFORMAÇÃO**

O plano de controle de acesso à informação é parte integrante da POSIN (Política de Segurança da Informação) da Secretaria de Estado da Administração do Governo do Estado de Santa Catarina. Composto por medidas, regras, diretrizes e normas a serem adotadas no que diz respeito a realização de auditorias internas com o intuito de medir a efetividade dos processos de controle de acesso à informação e identificar oportunidades de melhorias.

Seu principal objetivo é assegurar que apenas pessoas autorizadas tenham acesso aos recursos computacionais, além de gerenciar o acesso a equipamentos e ambientes críticos que armazenam informações.

**IDENTIFICAÇÃO DE USUÁRIOS**

* Estabelece os procedimentos necessários para garantir que seja possível a rastreabilidade dos acessos aos recursos computacionais.

**Registro de usuários de serviços de TI**

**Objetivo:**

* Identificar e registrar usuários de TI no banco de dados, bem como definir e registrar qual(ais) perfil(is) de acesso aos mesmos, assegurando acesso de usuário autorizado e prevenindo acesso não autorizado.

**Responsável:**

* Gerência de Recursos Humanos ou equivalente;
* Gerência de Tecnologia da Informação ou equivalente.

**Entradas:**

* Relação de novos usuários de TI;
* Relação de usuários ativos de TI com pedidos de alteração de perfis de acesso.

**Descrição das Atividades:**

* Identificar novos usuários de TI;
* Registrar novos usuários no banco de dados;
* Identificar usuários ativos de TI com pedidos de alteração de perfis de acesso;
* Registrar perfis de acesso no banco de dados.

**Saídas:**

* Registro de usuário de TI no banco de dados com identificação de seus perfis de acesso a sistemas e serviços de TI.

**Provimento de acesso aos usuários**

**Objetivo:**

* Associar usuários de TI aos sistemas, serviços e demais ativos de TI que terão direito de acesso.

**Responsável:**

* Gerência de Recursos Humanos ou equivalente;
* Gerência de Tecnologia da Informação ou equivalente.

**Entradas:**

* Relação de novos usuários de TI;
* Relação de usuários ativos de TI com pedidos de criação ou exclusão de direito de acesso a sistemas, serviços e demais ativos de TI.

**Descrição das Atividades:**

* Identificar novos usuários de TI;
* Identificar usuários ativos de TI com pedidos de concessão ou revogação de direito de acesso a sistemas, serviços e demais ativos de TI;
* Associar usuário de TI ao(s) sistema(s), serviço(s) e demais ativo(s) de TI para efetivação do direito de acesso aos mesmos.

**Saídas:**

* Registro de usuário de TI no banco de dados com informações de acesso a determinados sistemas, serviços e demais ativos de TI.

**Gerenciamento de credencial de acesso**

**Objetivo:**

* Gerenciar o ciclo de vida de concessão de acesso dos usuários de TI (concessão, ajuste e revogação) aos sistemas, serviços e demais ativos de TI, bem como controlar a geração de senhas de acesso e o acesso privilegiado dos usuários, assegurando acesso autorizado e prevenindo acesso não autorizado.

**Responsável:**

* Gerência de Recursos Humanos ou equivalente;
* Gerência de Tecnologia da Informação ou equivalente.

**Entradas:**

* Relação de usuários com perfis de acesso específicos.

**Descrição das Atividades:**

* Identificar novos usuários de TI com direito de concessão de acesso a sistemas, serviços e demais ativos de TI;
* Identificar usuários de TI com necessidade de alteração no direito de acesso a sistemas, serviços e demais ativos de TI;
* Identificar usuários de TI com necessidade de revogação do direito de acesso a sistemas, serviços e demais ativos de TI;
* Identificar usuários com direito de acesso privilegiado e validar junto aos gestores de unidades a manutenção do privilégio.

**Saídas:**

* Registro do usuário de TI atualizado no banco de dados com informação de senha de acesso, direitos de acesso e se possui acesso privilegiado a sistemas, serviços e demais ativos de TI.

**CONTROLE DE ACESSO LÓGICO**

* Define os procedimentos utilizados para proteger os ativos críticos contra tentativas de acesso não autorizadas.

**Controle de acesso à rede de dados**

**Objetivo:**

* Garantir o acesso à rede somente aos usuários autorizados e credenciados.

**Responsável:**

* Equipes de TI local.

**Entradas:**

* Informação de dispositivo de rede (switch), interface onde será conectado o equipamento, segmentação VLAN (se houver) e a lotação do usuário.

**Descrição das Atividades:**

* Identificar e informar o dispositivo e interface onde será conectado o computador.

**Saídas:**

* Dispositivo conectado e com acesso à rede de dados.

**Controle de acesso à rede sem fio**

**Objetivo:**

* Garantir o acesso à rede sem fio somente aos usuários autorizados e credenciados.

**Responsável:**

* Equipes de TI local.

**Entradas:**

* Relação de usuários e sua respectiva lotação para os quais deve ser liberado o acesso a rede sem fio.

**Descrição das Atividades:**

* Enviar a relação de usuários, e sua respectiva lotação, para liberação do acesso à rede sem fio;
* Adicionar os usuários nos respectivos grupos de liberação de acesso à rede sem fio de acordo com a lotação dos usuários.

**Saídas:**

* Usuários cadastrados no grupo do serviço de diretório com liberação de acesso à rede sem fio.

**Controle de acesso remoto**

**Objetivo:**

* Garantir o acesso remoto utilizando VPN - Virtual Private Network (Rede Privada Virtual) somente aos usuários autorizados e credenciados.

**Responsável:**

* Equipes de TI local;
* Gerência de Recursos Humanos ou equivalente.

**Entradas:**

* Usuários cadastrados no serviço de diretório.

**Descrição das Atividades:**

* Conceder ou excluir privilégio de acesso à VPN ao usuário, mediante necessidade para superior imediato.

**Saídas:**

* Usuário do serviço de diretório incluído no grupo com liberação de acesso à VPN.

Conforme orientação contida na Instrução Normativa n° 11/2021:

*Art. 13. À chefia imediata do agente público em regime de trabalho remoto, seja integral ou parcial, cabe:*

*II – solicitar às Gerências de Tecnologia e Comunicação ou unidades equivalentes o acesso remoto por VPN (Virtual Private Network), quando necessário.*

**Controle de acesso aos arquivos e diretórios**

**Objetivo:**

* Validar a manutenção das autorizações de acesso a diretórios e arquivos específicos aos usuários de TI.

**Responsável:**

* Equipes de TI local.

**Entradas:**

* Usuários cadastrados no serviço de diretório.

**Descrição das Atividades:**

* Verificar se todos usuários cadastrados no serviço de diretório continuam ativos e válidos;
* Verificar a existência de algum usuário de TI não cadastrado no serviço de diretório;
* Verificar, considerando lotação e atribuições, se os acessos a diretórios e arquivos específicos continuam válidos.

**Saídas:**

* Registros dos usuários de TI no serviço de diretório atualizados.

**Utilização de e-mail**

* O e-mail corporativo pertence ao Governo do Estado e pode ser monitorado quando este julgar necessário, sem prévio aviso.
* Somente devem ter acesso ao envio e recebimento de e-mail os colaboradores que necessitem deste recurso para suas atividades profissionais.
* O e-mail corporativo deve ser usado para fins profissionais e, excepcionalmente, poderão ocorrer trocas de mensagens de caráter não profissional por parte do colaborador, desde que sem abusos e sem prejuízos aos interesses públicos.
* O Governo do Estado não se responsabiliza pelo armazenamento de conteúdos pessoais em contas corporativas e tem o direito de revogar o acesso ou excluir estes documentos, caso for necessário;
* O colaborador não deve encaminhar e-mails recebidos cujo conteúdo não tenha relação com o trabalho.
* O colaborador não deve cadastrar o e-mail em formulários ou listas de discussão que não tenham relação com o trabalho.
* Os e-mails relacionados com o trabalho não devem ser enviados para destinatários não relacionados com a informação. Ex.: e-mail pessoal do colaborador.
* Sempre que possível, o colaborador deve evitar anexar arquivos ao e-mail. Especialmente no caso de e-mails internos, o colaborador deve dar preferência ao envio de links de arquivos ao invés de anexos.
* Quando fizer uso do e-mail pessoal o usuário deve ter cuidado ao abrir e-mails de origens desconhecidas ou baixar arquivos. O e-mail pessoal não deve ser usado para fins corporativos.

**CONTROLE DE ACESSO FÍSICO**

**Objetivo:**

* Prevenir o acesso não autorizado aos ambientes com acesso restrito, como exemplo o centro de processamento e armazenamento de dados, bem como evitar danos e interferências nos recursos de processamento e principalmente nas informações da organização.

**Responsável:**

* Equipes de TI local.

**Entradas:**

* Relação de ambientes com restrição de acesso.

**Descrição das Atividades:**

* Identificar pessoas com autorização de acesso aos ambientes restritos;
* Estabelecer protocolos de acesso restrito aos ambientes (quem acessar, quando acessar, porque acessar, etc.)
* Divulgar protocolos aos interessados.

**Saídas:**

* Protocolos de acesso restrito aos ambientes de processamento e armazenamento de informações.

**Perímetro externo**

* Recomenda-se ao perímetro externo possuir monitoramento de vídeo 24x7 e ser iluminado de modo a permitir bom monitoramento.
* Recomenda-se que a segurança externa, no período noturno e aos finais de semana, seja realizada por vigilantes devidamente treinados.
* Recomenda-se que o perímetro externo possua barreiras físicas que impeçam a entrada não autorizada de pessoas.

**Perímetro interno**

* Cada unidade e sede devem ter um mapeamento de ambientes físicos de segurança da informação, com a classificação de nível de segurança dos ambientes.
* Os ambientes administrativos devem possuir controle de acesso que restrinja o acesso de pessoas não autorizadas.
* As áreas de processamento de informação (data centers) devem ter níveis de segurança adequados à sua criticidade.
* Todas as manutenções executadas em ambientes que contenham ativos e passivos de TI devem ter o acompanhamento de um responsável da área de Tecnologia da Informação da unidade.
* Colaboradores devem permanecer com o crachá de identificação durante todo o período em que estiverem nas dependências do órgão.

**Acesso de visitantes**

* A entrada e saída de visitantes devem ser registradas na recepção, com data, hora e responsável interno pelo visitante.
* Visitantes devem utilizar identificação (crachá) durante todo o período da visita, sob responsabilidade do colaborador que o acompanha.
* Os visitantes, quando em ambientes administrativos, devem ser acompanhados por um colaborador durante toda a visita.

**Controle de chaves e alarmes**

* Os colaboradores que possuem acesso a chaves e alarmes externos devem assinar termo de responsabilidade específico.
* As liberações de uso de chaves e alarmes externos devem ser revisadas pelo menos a cada 12 meses.
* As chaves armazenadas devem possuir controle de acesso e protocolo para retirada e devolução.
* Somente colaboradores devidamente autorizados por sua gerência podem possuir chaves internas de seus setores.
* Ao ser transferido ou desligado o colaborador deve devolver todas as chaves que estão sob sua posse e seus direitos de alarmes devem ser desativados.

**AUDITORIA INTERNA**

**Objetivo:**

* Verificar possíveis inconsistências na execução dos processos de controle de acesso.

**Responsável:**

* Gerência de Tecnologia da Informação ou equivalente.

**Entradas:**

* Lista dos processos de controle de acesso, com seus respectivos detalhamentos (normas, protocolos, orientações, etc), associadas aos mesmos.

**Descrição das Atividades:**

* Analisar se as atividades de controle de acesso estão sendo executadas;
* Identificar atores de cada processo de controle de acesso;
* Analisar se o disposto nos normativos, protocolos, orientações, etc., estão sendo cumpridas pelos respectivos atores;
* Validar fiel cumprimento do disposto nos normativos, protocolos, orientações, etc.;
* Validar cumprimento da execução dos processos de controle de acesso.

**Saídas:**

* Relatório contendo inconsistências dos processos, normas, protocolos, etc.;
* Relatório descrevendo recomendações de melhorias em normas, protocolos, etc.

**Análise de perfis e direito de acesso aos usuários**

**Objetivo:**

* Analisar periodicamente os perfis dos usuários e respectivos direitos de acesso aos sistemas, serviços e demais ativos de TI.

**Responsável:**

* Gestores dos sistemas, serviços e demais ativos.

**Entradas:**

* Relação dos usuários de cada sistema, serviço e demais ativos.

**Descrição das Atividades:**

* Identificar o perfil de acesso de cada usuário de sistema, serviço e demais ativos;
* Conferir perfis de acesso;
* Identificar usuários com direito de acesso privilegiado;
* Ratificar privilégio de acesso;
* Realizar análise de LOGs, permitindo a geração de relatórios e emissão automática de alertas de eventos que possam representar riscos.

**Saídas:**

* Registros dos usuários atualizados.