SEGURANÇA DA INFORMAÇÃO

MACROPROCESSO DE CONTROLE DE ACESSO

Data: 10/09/2020

Versão 3.0

HISTÓRICO DE ALTERAÇÕES

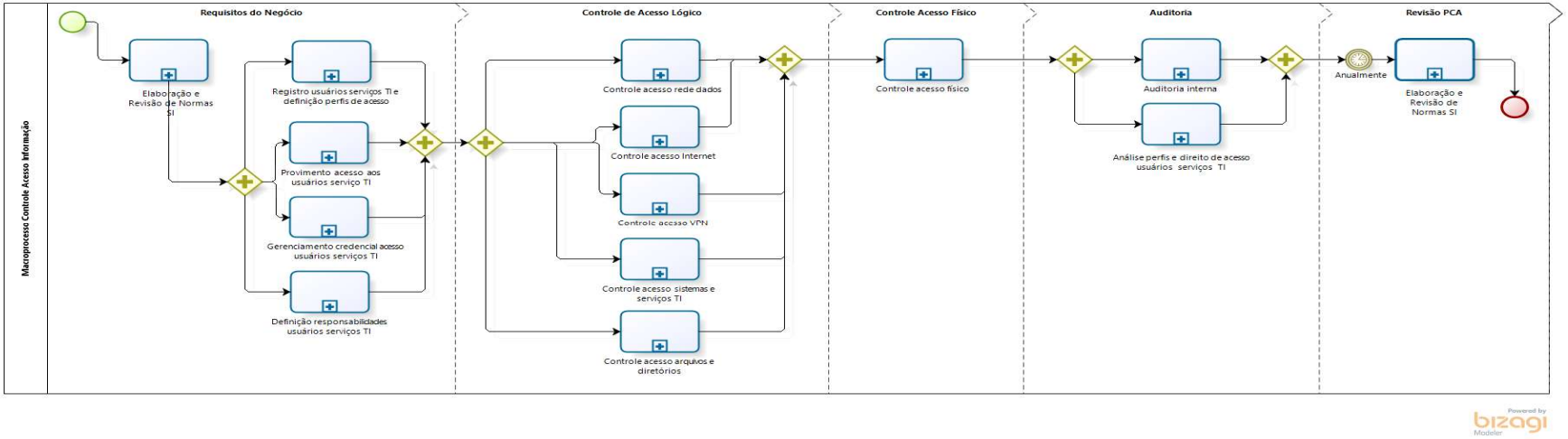
DOCUMENTO		
Descrição	Documentação dos processos de Segurança da Informação	
Objetivo	Este documento descreve os processos componentes do Macroprocesso de Controle de Acesso do PJSC	
Responsável	**Nome/Matrícula** Rinaldo Feldmann - 2160	**Criado em** 13/08/2020
Setor Secretaria de Segurança da Informação e Gestão de Riscos - SSIGR		

V E R S I O N A ME N TO S			
Versão	Data	Autor	Descrição
1.0	13/08/2020	Rinaldo Feldmann	Criação do Documento
2.0	04/09/2020	Rinaldo Feldmann	Alterações propostas pela equipe de Segurança da Informação
3.0	10/09/2020	Rinaldo Feldmann	Validação da SSIGR

SUMÁRIO

MACROPROCESSO DE CONTROLE DE ACESSO

Diagrama do Processo



PAPÉIS E RESPONSABILIDADES

Papéis		Responsabilidades
Comitê de Governança de Tecnologia da Informação (CGOVTI)	Comitê multidisciplinar formado por magistrados e servidores, vinculado à Presidência, de natureza deliberativa e de caráter permanente.	- aprovar estratégias, planos, processos e decidir sobre ações de melhorias e correções em relação ao controle de acesso; e - decidir, ouvido o Comitê Gestor de Segurança da Informação, os casos omissos.
Comitê Gestor de Segurança da Informação (CGSI)	Comitê multidisciplinar, vinculado ao CGOVTI, formado por juiz auxiliar do Núcleo Administrativo e servidores da área de tecnologia da informação.	- propor ajustes, aprimoramentos e modificações no macroprocesso de controle de acesso; - deliberar sobre controles, processos e procedimentos de controle de acesso; - acompanhar a estratégia, processos, projetos e iniciativas corporativas de controle de acesso, zelando por sua qualidade e efetividade; - propor o planejamento e a alocação de recursos no que tange ao controle de acesso; e - atuar como instância consultiva da Presidência do Tribunal nas questões relativas ao controle de acesso;
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Setor responsável pela normatização e atualização das normas de segurança da informação, em conjunto com as demais áreas competentes.	- coordenar a elaboração do desenho e detalhamento de processos componentes do macroprocesso de controle de acesso, bem como normatização correlata; e - subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes ao controle de acesso.
Equipe Multisetorial de Segurança da Informação	Grupo formado por representantes de cada divisão da DTI com a responsabilidade de analisar, propor melhorias e validar processos, projetos e ações relativas à implementação do SGSI.	- propor ao Comitê Gestor de Segurança da Informação as diretrizes estratégicas de controle de acesso; - propor projetos e iniciativas para o aperfeiçoamento do controle de acesso; - definir a metodologia e as ferramentas a serem utilizadas na condução da Gestão de

		Continuidade de Negócios; - garantir a operacionalização e a exequibilidade dos planos; - avaliar a eficácia dos planos, sugerindo a correção de falhas, com base no registro de incidentes;

CONTROLE DE EXECUÇÃO

Controle	Método de execução	Frequência
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Execução do processo de Elaboração e Revisão de normas de Segurança da Informação com objetivo de identificar normativos a serem elaborados necessários para a implementação do macroprocesso de controle de acesso	Imediato
	Execução do processo de Elaboração e Revisão de normas de Segurança da Informação com objetivo de identificar necessidade de revisão da Política de controle de acesso	Anual
Divisões DTI	Realização de auditorias internas com o intuito de medir a efetividade dos processos componentes do macroprocesso de controle de acesso e identificar oportunidades de melhorias	Semestral

FERRAMENTAS

PDTI	Plano Diretor de TI
PETI	Planejamento Estratégico de TI - indicadores de desempenho do PETI

DESCRIÇÃO DAS ATIVIDADES

REQUISITOS DO NEGÓCIO

Registro de usuários de serviços de TI e definição de perfis de acesso

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:

- Diretoria de Gestão de Pessoas;
- Divisão de Sistemas Administrativos.

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 de serviço de TI

Objetivo:

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

Responsável:

- Diretoria de Gestão de Pessoas;
- Divisão de Sistemas Administrativos;
- Gestores da Informação.

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 usuários de serviços de TI

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:

- Divisão de Suporte e Gestão de Ativos de TI;
- TSI'S;
- Gestores da Informação.

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 do PJSC, 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.

Definição de responsabilidades dos usuários de serviços de TI

Objetivo:

- Orientar usuários de TI das suas responsabilidades pela proteção de sua senha de acesso aos sistemas, serviços e demais ativos de TI.

Responsável:

- Divisão de Sistemas Administrativos;
- Divisão de Sistemas Judiciais;
- Divisão de Infraestrutura;
- Divisão de Redes de Comunicação;
- Divisão de Suporte e Gestão de Ativos de TI;
- Divisão de Apoio Judiciário da Diretoria de Suporte à Jurisdição de 1º Grau;
- Diretoria-Geral Judiciária.

Entradas:

- Rol de responsabilidades dos usuários por sistema, serviço e demais ativos de TI.

Descrição das Atividades:

- Descrever responsabilidade dos usuários por perfil de acesso aos sistemas, serviços e demais ativos de TI;
- Publicar responsabilidades no Portal de TI;
- Publicar responsabilidades no Portal do servidor.

Saídas:

- Responsabilidades publicadas.

CONTROLE DE ACESSO LÓGICO

Controle de acesso à rede de dados

Objetivo:

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

Rede lógica

Responsável:

- Divisão de Redes de Comunicação;
- Técnicos de Suporte de Informática (TSI's).

Entradas:

- Informação de switch e interface do switch onde será conectado o equipamento do usuário e a lotação do usuário.

Descrição das Atividades:

- Identificar e informar o switch e qual interface do switch onde será conectado o computador;
- Identificar a VLAN de acesso relativa ao equipamento do usuário;
- Cadastrar a interface do switch na VLAN identificada anteriormente.

Saídas:

- Interface do switch configurado na VLAN correta.

Rede Wireless

Responsável:

- Divisão de Redes de Comunicação.

Entradas:

- Relação de usuários, e sua respectiva lotação, para os quais deve ser liberado o acesso a rede Wireless.

Descrição das Atividades:

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

Saídas:

- Usuários cadastrados no grupo do AD com liberação de acesso a rede Wireless.

Controle de acesso à internet

Objetivo:

- Garantir o acesso à internet somente aos usuários autorizados e credenciados.

Responsável:

- Divisão de Redes de Comunicação;
- Técnicos de Suporte em Informática (TSIs).

Entradas:

- Usuário do AD.

Descrição das Atividades:

- Criação de um novo usuário onde o sistema de ciclo de vida do usuário já concede o privilégio de acesso à internet em nível comum;
- Chamado da central de serviços solicitando a liberação de acesso a algum site ou o bloqueio de acesso;
- Conceder o nível de privilégio de acesso à internet adequado ao usuário, mediante justificativa de necessidade para desempenho do trabalho ou mediante solicitação do superior imediato.

Saídas:

- Usuário do AD incluído em um dos grupos com níveis de privilégios de acesso à internet: bloqueado, comum, completo ou limitado.

Controle de acesso à VPN

Objetivo:

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

Responsável:

- Divisão de Redes de Comunicação;
- Técnicos de Suporte em Informática (TSIs).

Entradas:

- Usuário do AD.

Descrição das Atividades:

- Criação de um novo usuário onde o sistema de ciclo de vida do usuário já concede o privilégio de acesso à VPN;
- Chamado da central de serviços solicitando liberação ou bloqueio de acesso à VPN;
- Conceder ou excluir privilégio de acesso à VPN ao usuário, mediante necessidade para o desempenho do trabalho ou mediante solicitação do superior imediato.

Saídas:

- Usuário do AD incluído no grupo com liberação de acesso à VPN.

Controle de acesso aos sistemas e serviços de TI

Objetivo:

- Prevenir o acesso não autorizado aos sistemas e serviços de TI.

Responsável:

- Gestor do sistema ou serviço de TI.
- Divisão de Sistemas Administrativos;
- Divisão de Sistemas Judiciais;
- Divisão de Infraestrutura;
- Divisão de Redes de Comunicação;
- Divisão de Suporte e Gestão de Ativos de TI.

Entradas:

- Relação de usuários autorizados a acessar sistemas e serviços de TI;
- Relação de sistemas e serviços de TI.

Descrição das Atividades:

- Validar perfis e autorização de todos os usuários ativos com acesso aos sistemas e serviços de TI;

- Identificar usuários a terem perfis alterados e com necessidade de alteração da concessão ou remoção de acesso;
- Encaminhar relação de usuários com alterações de registro para a Seção de Atendimento ao usuário da Divisão de Suporte e Gestão de Ativos de TI;
- Identificar se o acesso aos sistemas e serviços com necessidade de acesso por senha estão sob o controle de procedimento seguro;
- Identificar se o acesso ao código-fonte dos programas está sob restrito aos analistas e programadores envolvidos nos projetos (considerar deliberação do CGOVTI de 05/06/2020- Ata n. 02 - Permitir o acesso direto ao banco de dados exclusivamente por meio da base *slave* (cópia).

Saídas:

- Alteração dos registros de usuários no banco de dados com perfis alterados e com alteração da concessão ou remoção de acesso.

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:

- TSI's;
- Divisão de Suporte e Gestão de Ativos de TI;
- Gestores de unidades administrativas do PJSC.

Entradas:

- Usuários cadastrados ferramenta da Microsoft utilizada para o gerenciamento de usuários de rede, denominada Active Directory (AD).

Descrição das Atividades:

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

Saídas:

- Registros dos usuários de TI no AD atualizados.

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 das informações e principalmente nas informações da organização.

Responsável:

- Divisão de Infraestrutura;
- Divisão de Redes de Comunicação.

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;
- Publicar protocolo no Portal da TI.

Saídas:

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

AUDITORIA INTERNA

Objetivo:

- Verificar possíveis inconsistências no cumprimento dos normativos, protocolos, orientações, etc., bem como na execução dos processos componentes do macroprocesso de controle de acesso.

Responsável:

- Auditoria Interna do PJSC.

Entradas:

- Lista dos processos componentes do macroprocesso de controle de acesso, com seus respectivos detalhamentos e normas, protocolos, orientações, etc., associadas aos mesmos.

Descrição das Atividades:

- Analisar se as atividades componentes de cada processo componente do macroprocesso de controle de acesso estão sendo executadas;
- Identificar atores de cada processo do componente do macroprocesso 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 componentes do macroprocesso de controle de acesso.

Saídas:

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

Análise de perfis e direito de acesso aos usuários de serviços de TI

Objetivo:

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

Responsável:

- Auditoria Interna do PJSC;
- Gestores dos sistemas, serviços e demais ativos de TI.

Entradas:

- Relação dos usuários de cada sistema, serviço e demais ativos de TI;

Descrição das Atividades:

- Identificar o perfil de acesso de cada usuário de sistema, serviço e demais ativos de TI;
- Ratificar perfis de acesso aos sistemas, serviços e demais ativos de TI;
- Identificar usuários com direito de acesso privilegiado;
- Ratificar privilégio de acesso.

Saídas:

- Registros dos usuários de TI atualizados.