Política gerais da tecnologia da informação na SteelMast

Este documento tem como finalidade apresentar as principais políticas na gestão de ativos e dados, na tecnologia da informação utilizada pela SteelMast e suas filiais. Este é um documento com informações e dados internos que deve ser mantido em sigilo, salvo em casos de comprovações a um analista em seu comprimento de auditoria interna.

Para facilidade no seu entendimento, este documento foi dividido em capítulos e sessões conforme apresentadas do índice a seguir. A data da última atualização pode ser consultada no rodapé de qualquer página deste documento, juntamente com o número da página atual e seu total.

Índice

1 POLÍTICA DE GESTÃO DE ATIVOS

2020, através do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena

O objetivo desta política é garantir que os ativos de informações seja identificadas adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Para manter a segurança e continuidade do negócio da SteelMast, em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para um maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de riscos da organização. Auxiliando também na recuperação de incidentes.

Os ativos de informação da SteelMast deve ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um "dono", no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

1.1 Escopo

Esta política se aplica a todos os ativos de informação da SteelMast, incluindo ativos fora da SteelMast armazenados em um serviço de nuvem. Ativos de informações neste contexto, incluem documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistema e internet, planos, guias, programas de computadores, servidores, computadores, e-mails, arquivos pessoais e compartilhados, bancos de dados, desenhos técnicos e conteúdo da web específicos.

A classificação dos ativos de informação e o escopo desta política serão revisados anualmente.

1.2 Termos e definições

- ATIVOS DE INFORMAÇÃO - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

- INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicidade indevida de informação protegida de algum ativo de informação crítica ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

1.3 Referência legal e de boas práticas

Orientação	**Secção**
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Decreto Nº 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Incisos III, IV, VIII e XI CAPÍTULO VI - Seção IV - Art.15

Framework de segurança cibernética do CIS 8	Salvaguarda 1,2 e 3
Framework Information Technology Infrastructure Library - ITIL, v.4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR	Art.12 Inciso IV, alínea d
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo II
Lei Nº 12.527/2011 - Lei de Acesso à Informação (LAI)	Em sua íntegra
Lei Nº 13.709/2018 - Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I - Art.46, Seção II Art.50
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	Em sua íntegra.

1.4 Declarações da política

Dos princípios gerais

I. A Política de Gestão de Ativos de informação deve estar alinhada com à Política de Segurança da Informação da SteelMast.

II. A Política da Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

III. O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos â segurança da informação.

IV. As rotinas de inventário e mapeamento de ativos de informações deve ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

V. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

VI. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

Os seguintes ativos de informação deve ser considerados no processo de mapeamento de ativos de informação:

I. Ativos físicos;

II. Bancos de dados;

III. Dispositivos móveis;

IV. Hardwares;

V. Mídias removíveis;

Softwares.

Diretrizes:

1. Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

    a. A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização.

    b. A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.

    1. O inventário também deverá incluir atualizações ou remoções do sistema de informação.

2. Das responsabilidades do proprietário do processo.

    a. Identificar potenciais ameaças aos ativos de informação;

    b. Identificar vulnerabilidades dos ativos de informação;

    c. Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

    d. Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação;

    e. Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos;

    f. Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados;

g. Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

3. Criticidade do ativo de informação

   a. A criticidade dos ativos de informação críticos da organização é determinado pelo:

      i. Requisitos legais;

      ii. Pelo valor financeiro;

      iii. Pelo potencial de agregar valor ao negócio;

      iv. Por sua vida útil.

4. Classificação das informações:

   a. Todos os ativos de informação devem ser classificados de acordo com sua criticidade.Todos os ativos de informação devem ser classificados de acordo com sua criticidade.

   b. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação da SteelMast devem ser classificados de acordo com a legislação pertinente, podendo ser classificado em uma das seguintes categorias:

      i. **Ultrassecreta**: São passíveis de classificação como ultrassecretos, dentre outros, dados, informações ou documentos referentes à soberania e à integridade territorial nacionais, a planos e operações, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano

excepcionalmente grave à segurança da sociedade ou do Estado.

ii. **Secreta**: São passíveis de classificação como secretos, dentre outros, dados, informações ou documentos referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança da SteelMast, da sociedade ou do Estado.

iii. **Reservada**: São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse da SteelMast, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da SteelMast, da sociedade ou do Estado.

c. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de informações usados pela organização.

5. Manipulação de mídia:

a. A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.

b. A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve

ser descartada com segurança, usando os procedimentos apropriados.

c. A mídia contendo informações confidenciais e internas da SteelMast devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

6. Uso aceitável:

a. Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

b. Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis:

i. Uso do computador e dos sistemas de informação;

ii. Uso de softwares e dados;

iii. Uso da Internet e e-mail;

iv. Uso do telefone;

v. Uso de equipamentos e materiais de escritório.

c. Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis

1.5 Não conformidade

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Processo Administrativo disciplinar de acordo com a legislação aplicável;
2. Exoneração;
3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.

2 POLÍTICA DE CONTROLE DE ACESSO

A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da SteelMast, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação da SteelMast.

2.1 Escopo

Esta Política se aplica a todas as informações, cuja a SteelMast seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Especificamente, inclui:

- Todos os funcionários, sejam servidores efetivos ou temporários, da SteelMast.
- Todos os contratados e terceiros que trabalham para a SteelMast.

- Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação da SteelMast.

2.2 Termos e definições

- 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;

- CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

2.3 Referência legal e de boas práticas

Orientação	**Secção**
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso XI CAPÍTULO VI - Seção IV – Art.15
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea f
Norma Complementar nº 7/IN01/DSIC/GSIPR	Item 7
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de

	Auditoria Páginas 30-32
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação	Itens 9 – 11.2.9 (Páginas 23 - 47)
CIS V8	CAPÍTULO 6
Guia do Framework de Segurança – LGPD	Páginas 24 - 26
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

2.4 Declarações da política

Acesso lógico

Art. 1º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pelo setor da tecnologia da informação (TI), baseado nas responsabilidades e tarefas de cada usuário.

I. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

II. Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na SteelMast.

III. O acesso remoto deve ser realizado por meio da plataforma oferecia pelo setor de TI, após as devidas autorizações.

Conta de acesso lógico e senha

Art. 2º Para utilização das estações de trabalho da SteelMast, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pelo setor de TI, mediante solicitação formal pelo titular da unidade do requisitante.

I. O formulário de solicitação de acesso se encontra disponível para preenchimento na Intranet da SteelMast.

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para o setor de TI que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 3º O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo setor de TI quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 4º O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, joão.silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, o setor de TI realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 5º O padrão adotado para o formato da senha é o definido pelo setor de TI, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (login) de acesso à Rede Local deve seguir as regras de:

   a. Possuir tamanho mínimo de seis caracteres, sendo obrigatório o uso de letras e números;

   b. Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

   c. Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

   d. Não utilizar termos óbvios, tais como: nome, senha, usuário, password ou admin;

   e. Não reutilizar as últimas 06 (seis) senhas.

II. O setor de TI fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 6º As senhas de acesso serão renovadas a cada 90 (noventa) dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

Bloqueio, desbloqueio e cancelamento da conta de acesso

I. Art. 7º A conta de acesso será bloqueada nos seguintes casos: Após 3 (três) tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pela SteelMast ou descumprimento da Política de Segurança da Informação – POSIN e normas correlatas em vigência.

IV. Após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

Art. 8º O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário ao setor de TI.

Art. 9º Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do setor de RH.

Art. 10º A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Movimentação interna

Art. 11º Quando houver mudança do usuário para outro setor, os direitos de acesso à Rede Local devem ser readequados, conforme solicitação do novo superior imediato ou do setor de RH.

Parágrafo único. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou do setor de RH.

Conta de acesso biométrico

Art. 12º A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multi fatores.

Parágrafo único. A SteelMast deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

Administradores

Art. 13º A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente os técnicos do setor de TI, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o setor de TI, que poderá negar os casos em que entender desnecessária a utilização.

III. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal do setor de TI

IV. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

V. A identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

VI. Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador

para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

VII. Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do setor responsável por meio do setor de TI.

Responsabilidades

Art. 14º É de responsabilidade do superior imediato do usuário comunicar formalmente ao setor de RH e ao setor de TI o desligamento ou saída do usuário da SteelMast para que as permissões de acesso à Rede Local sejam canceladas.

Art. 15º Caberá ao setor de RH da SteelMast a comunicação imediata ao setor de TI sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 16º É responsabilidade do setor de RH da SteelMast a comunicação imediata ao setor de TI sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

I. Os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

II. Nenhum técnico de empresa terceira terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores da SteelMast sem a devida supervisão do setor de TI.

Art. 17º É de responsabilidade do setor de TI o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como

bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica da SteelMast.

Art. 18º O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade da SteelMast.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 19º O usuário deve informar ao setor de TI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 20º É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a SteelMast, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII. Assinar o Termo de Responsabilidade quanto a utilização da respectiva conta de acesso.

Disposições gerais

Art. 21º Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários ao setor de TI.

Art. 22º Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o setor de TI fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o ator da quebra de segurança for um usuário, o setor de TI comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. Ações que violem a POSIN ou que quebrem os controles de Segurança da Informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

III. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIN.

IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação - CSI da SteelMast.

3 POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo departamento de TI e formalmente definidos como de necessária salvaguarda na SteelMast, para se manter a continuidade do negócio.

No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

3.1 Escopo

- Esta política se aplica a todos os dados no âmbito da SteelMast, incluindo dados fora da SteelMast armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem projetos em andamento e finalizados, bancos de dados e documentos operacionais diversos. A definição de dados críticos e o escopo desta política de backup serão revisados anualmente.
- Os serviços de TI críticos da SteelMast devem ser formalmente elencados pelo Comitê de Gestão de Tecnologia da Informação da organização.
- Já ficam previamente estabelecidos os dados e informações atuais, como serviços críticos da SteelMast.
- Esta política se aplica a funcionários que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que

acessam e usam na SteelMast sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da SteelMast.

- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

- A salvaguarda dos dados em formato digital pertencentes a serviços de TI da SteelMast mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

3.2 Termos e definições

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;

CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos,

magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

3.3 Referência legal e de boas práticas

Orientação	**Secção**
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15

Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 11 (Data Recovery Capabilities)
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemasde gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

3.4 Declarações da política

Dos princípios gerais

I. A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação da SteelMast.

II. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

III. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

IV. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

V. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

VI. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

VII. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

VIII. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

IX. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados

I. Os backups dos serviços de TI críticos da SteelMast devem ser realizados ao menos uma vez ao dia onde existe a modificação de arquivos ou sistemas;

II. Os serviços de TI críticos da SteelMast devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados, permanecerá um backup dos últimos 7 dias, das últimas 4 semanas e cada um dos últimos 12 meses. Sempre havendo pelo menos um backup. (2 meses onedrive)

III. Os serviços de TI NÃO críticos da SteelMast devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida de 1 mês.

IV. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

V. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

VI. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos responsáveis, com a anuência prévia e formal dos mesmos, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos: Escopo (dados digitais a serem salvaguardados); Tipo de backup (completo, incremental, diferencial); Frequência temporal de realização do backup (diária, semanal, mensal, anual); Retenção; RPO; RTO.

VII. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao responsável pelo Backup. A aprovação para execução da alteração depende da anuência do responsável.

VIII. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

IX. Tipo de backup: incremental e diferencial com desduplicação de arquivos.

Do uso da rede

I. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da SteelMast, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da SteelMast.

II. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

III. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados da SteelMast.

Do transporte e armazenamento

I. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados: A criticidade do dado salvaguardado; O tempo de retenção do dado; A probabilidade de necessidade de restauração; O tempo esperado para restauração; O custo de aquisição da

unidade de armazenamento de backup; A vida útil da unidade de armazenamento de backup.

II. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

III. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

IV. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

V. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 30 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

VI. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

VII. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Dos testes de backup

I. Os backups serão verificados periodicamente, com um teste fixo uma vez ao mês.

II. Os *logs* de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup uma vez na semana.

III. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.

IV. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.

V. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

VI. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.

VII. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

VIII. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo setor de TI.

Procedimento de restauração de backup

I. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

   a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de um e-mail.

b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

c. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

d. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

II. O cronograma de restauração de dados:

a. O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, é proporcional ao volume de dados necessários para o restore. A cada 1GB de dados, o tempo de restauração é de 5 minutos. Esta estimativa é do tempo de atendimento do departamento de TI juntamente com as empresas terceirizadas de backup, não contemplando o tempo antes ou após o pedido a equipe.

b. Backups externos serão disponibilizados em aproximadamente 2 horas de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;

c. Backups externos serão disponibilizados em aproximadamente 5 horas de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

Do Descarte da Mídia

I. A mídia de backup será retirada e descartada conforme descrito neste documento:

   a. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

   b. A TI garantirá a destruição física da mídia antes do descarte.