PREFEITURA DE SÃO PAULO

MANUAL DE ORIENTAÇÃO SOBRE GESTÃO DE RISCOS NO SETOR TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO EM SEGES

1ª EDIÇÃO - 2026

PREFEITURA DE
SÃO PAULO

PREFEITURA DE SÃO PAULO

Prefeito
Ricardo Nunes

SECRETARIA MUNICIPAL DE GESTÃO

Secretária
Marcela Arruda

Secretária Adjunta
Regina Silverio

Chefe de Gabinete
Thaís Rodrìgues

COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Wagner Santana Silveira

REDAÇÃO
Davi Giugno
João Victor Silva
Rafael da Matta

DIAGRAMAÇÃO
Bianca Abreu
Carolina Teixeira

REVISÃO
Roseli Andrade Pires

SUMÁRIO

GLOSSÁRIO

ABNT NBR ISO nº 31000:2018: A ISO 31000 é conhecida como a norma da gestão de risco. Seu objetivo é evitar ameaças que prejudiquem a segurança do trabalho.

Acesso: Refere-se a um nível de funcionalidade de um serviço ou dados a que o usuário possui direitos de acesso e uso.

Antivírus: O antivírus é um software que identifica e protege os dispositivos de malwares, também conhecidos como vírus.

APIs: Interface de programação de aplicações.

Backup: Termo utilizado para uma atividade que consiste em realizar cópias de segurança de dados digitais de um dispositivo.

Checklist: Uma lista de verificação

COTIC: Coordenadoria de Tecnologia da Informação e Comunicação.

HDs e SSDs: unidade de armazenamento de dados.

LGPD: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

Logins: Perfis de acessos.

Logs: Arquivos de texto nos quais são registradas informações diversas, geralmente seguindo a cronologia dos eventos acontecidos;

Malware: Malware é qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores.

No-Breaks: O nobreak é um equipamento que protege e mantém em funcionamento dispositivos eletroeletrônicos em situações de oscilação ou ausência da rede elétrica.

Phishing: Phishing é uma técnica de engenharia social usada para enganar usuários de internet usando fraude eletrônica para obter informações confidenciais.

Prodam: Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo, de economia mista, é a parceira tecnológica da Prefeitura de São Paulo e integradora estratégica de soluções inovadoras de tecnologia da informação e da comunicação.

PSI: Refere-se à portaria da Política de Segurança da Informação, da Secretaria Municipal de Gestão.

SEGES: Refere-se a Secretaria Municipal de Gestão.

SLA: Acordo de Nível de Serviço.

TIC ou TI: Refere-se a tecnologia da informação e comunicação.
Vírus: Um vírus de computador é um tipo de programa malicioso que se propaga através de computadores e dispositivos conectados em rede, por meio de downloads de arquivos infectados, anexos de e-mail maliciosos, sites comprometidos, dispositivos de armazenamento e outros tipos de arquivos infectados.

Wi-Fi: Wi-Fi é uma tecnologia de rede sem fio que permite que computadores, dispositivos móveis e outros equipamentos (impressoras e câmeras de vídeo) se conectem à Internet.

INTRODUÇÃO

Este documento é derivado da PSI de SEGES, conforme estabelecido e referenciado em seu Art 2º, e tem por fim complementá-la em pontos relativos a riscos cotidianos de TIC em SEGES.

Este documento está igualmente ligado ao **Manual de Orientação de Acessos de Tecnologia da Informação e Comunicação em SEGES** e ao **Manual de Orientação sobre Plano de Continuidade de Negócio no Setor Tecnologia da Informação e Comunicação em SEGES**, documentos igualmente derivados da Política de Segurança da Informação (PSI) de SEGES.

1. DEFINIÇÃO DE RISCO E DE GESTÃO DE RISCO

Conforme define a norma ABNT NBR ISO nº 31000:2018, “risco” é o “efeito da incerteza nos objetivos”. A “gestão de riscos”, por sua vez, é o conjunto de “atividades coordenadas para dirigir e controlar uma organização no que se refere aos riscos”.

2. MAPEAR RISCOS

Os riscos, em qualquer negócio, podem ser mapeados e se possível, quantificados quanto aos seus impactos, sejam estes econômicos, legais, ambientais, tecnológicos, de segurança, políticos, etc.

Após o devido mapeamento dos riscos, podem ser montadas estratégias para lidar com eles, seja aceitando-os, compartilhando-os, transferindo-os, reduzindo-os ou mesmo evitando-os. Desta forma, o negócio ficará menos vulnerável a tais riscos, elevando suas probabilidades de continuidade e sustentabilidade em um cenário cada vez mais complexo. E com a área de TI, não é diferente.

3. MAPEANDO RISCOS DE TI

A área de TI é de fundamental importância hoje em dia, para grande parte dos negócios, mesmo para aqueles que não oferecem produtos e serviços de TI, sendo apenas usuários de recursos de TIC para fins de armazenamento e processamento de dados, ou para facilitar transações comerciais e rastreamento de produtos, por exemplo.

Um exemplo de risco de TI que pode acometer qualquer negócio é o vazamento de informações sensíveis e sigilosas que estejam em sistemas de informação ou em bancos de dados. Os riscos financeiros e jurídicos de tais vazamentos podem ser elevadíssimos, a depender do que exatamente foi vazado, da natureza do negócio, das leis vigentes na jurisdição onde ocorreu o problema e de quem foi afetado. Tudo isso para não falar nos riscos para a reputação do negócio, que podem ser gigantescos, especialmente em empresas do setor financeiro, em plataformas de mídias sociais e mesmo no setor público.

Diante desse cenário, o processo de mapeamento e mensuração de riscos de TI torna-se imprescindível. Este manual apresenta um roteiro estruturado para identificar, avaliar e tratar riscos de TI, com base nas práticas adotadas na SEGES e considerando as especificidades da gestão pública municipal.

3.1 Identificações dos Riscos

- Revisar lições aprendidas;
- Checklist de riscos;
- Lista de riscos;

3.2 Avaliações dos Riscos

- Reunião de riscos;
- Matriz de probabilidade X impacto – esta terá bastante importância para nós.

3.3 Priorização

- Priorizar riscos para obter um repositório com o que deve ser feito;
- Criar um processo de priorização de riscos.

3.4 Estratégia

- Desenvolver estratégia apropriada para lidar com o risco;
- A resposta vai depender da probabilidade e impacto;
- Deve ser uma resposta proativa

3.5 Comunicação

- Comunicar os resultados para os stakeholders apropriados;

4. MATRIZ DE RISCO – O QUE É E COMO CONSTRUIR

No momento de avaliar o risco para um determinado evento, tomamos as duas dimensões que o evento tem: sua Probabilidade (de ocorrência dentro de um determinado período) e seu Impacto (medida do potencial comprometimento dos objetivos e resultados da organização avaliada, quando o evento acontece).

O passo seguinte é criar a chamada Matriz de Risco, que é uma matriz cujas linhas e colunas combinem as dimensões de Impacto e de Probabilidade, fornecendo assim os níveis de Risco associados a cada combinação particular de Impacto e Probabilidade. Lembramos sempre que a variável Impacto tem maior peso do que a Probabilidade, pois faz todo sentido que um evento de baixa probabilidade, mas com alto impacto, seja bem mais preocupante para a organização do que um evento de alta probabilidade, porém com baixo impacto.

Importante também é lembrar que tais matrizes de risco são mais qualitativas do que quantitativas, pois nem sempre é simples traduzir em valores numéricos o risco, ou criar fórmulas matemáticas para calculá-lo. Muitas vezes, temos de nos guiar pelo bom senso e pela experiência, como mostramos nas duas tabelas abaixo, com sugestões de Escala de Probabilidade e de Escala de Impacto.

Escala de Probabilidade – Uma Sugestão

Escala	Descrição
Muito Baixa	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
Baixa	O histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo
Média	Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte
Alta	Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerão nesse horizonte
Muito Alta	Ocorrência quase garantida no prazo associado ao objetivo.

Escala de Impacto – Uma Sugestão

Escala	Descrição
Muito Baixo	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado
Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
Médio	Compromete razoavelmente o alcance do objetivo/resultado.
Alto	Compromete a maior parte do atingimento do objetivo/resultado
Muito Alto	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.

5. MATRIZ DE RISCOS QUALITATIVA

Com as escalas de Probabilidade e de Risco propostas no item 4 acima, construímos uma Matriz de Riscos. Esta última pode ser qualitativa, isto é, uma matriz que classifique os riscos em categorias como Baixo, Médio, Alto ou Extremo, ou pode ser uma matriz quantitativa, composta de números gerados por fórmulas matemáticas combinando valores numéricos atribuídos a diferentes níveis de Probabilidades e de Impacto. No que se segue, é construída uma matriz de risco qualitativa, a partir das dimensões de Impacto (nas linhas) e de Probabilidade (nas colunas).

Tabela de Matriz de Risco – Um Exemplo de Construção

Muito Alto	**Risco Alto**	**Risco Alto**	**Risco Extremo**	**Risco Extremo**	**Risco Extremo**
Alto	**Risco Moderado**	**Risco Moderado**	**Risco Alto**	**Risco Extremo**	**Risco Extremo**
Médio	**Risco Baixo**	**Risco Moderado**	**Risco Alto**	**Risco Alto**	**Risco Alto**
Baixo	**Risco Baixo**	**Risco Baixo**	**Risco Moderado**	**Risco Moderado**	**Risco Moderado**
Muito Baixo	**Risco Baixo**	**Risco Baixo**	**Risco Baixo**	**Risco Baixo**	**Risco Moderado**
Impacto ^ / Probabilidade. >	**Muito Baixa**	**Baixa**	**Média**	**Alta**	**Muito Alta**

Reforçamos aqui que a tabela acima é apenas um exemplo de matriz de risco possível, sendo que cada organização pode e deve ajustar a matriz de risco à sua realidade. Usaremos a matriz acima no restante deste documento, a título de exemplo.

Vale lembrar que essa classificação é para os riscos ANTES das medidas de tratamento, ou seja, é o risco pré-tratamento ou risco inerente. Voltaremos a este ponto na seção 08.

6. EXEMPLOS PRÁTICOS DE RISCOS DE TIC EM SEGES

Aqui citaremos alguns exemplos de riscos que podem se materializar no dia a dia da SEGES. As medidas de prevenção são apenas sugestões, e poderão ser revisadas e aprimoradas com o tempo. Além do mais, as medidas de tratamento, nos casos realmente graves, que tenham potencial de paralisar atividades críticas da Secretaria, constarão de um futuro documento de Plano de Continuidade de Negócios, a ser elaborado em COTIC. Para casos menos graves, podemos sugerir medidas de tratamento no presente documento.

6.1 Um usuário esquece a senha de acesso à rede corporativa

É um evento com muito alta probabilidade de ocorrência, sendo quase diário em SEGES. No entanto, costuma ter solução relativamente rápida e seu impacto fica restrito às tarefas do usuário e eventualmente de colegas que dependam de seu trabalho, então o impacto é, na pior das hipóteses, apenas baixo. Na matriz acima, o risco correspondente é um Risco Baixo.

Forma de Prevenção: Guardar a senha de acesso em local seguro.

Forma de Tratamento: Abertura de chamado para reinicialização da senha esquecida.

6.2 Vazamento de dados confidenciais ou pessoais sensíveis de propriedade da Secretaria

É um evento com probabilidade relativamente baixa de ocorrência em SEGES. Porém, caso aconteça, as consequências poderão ser muito graves, a depender do que exatamente foi vazado. Dados de perícias médicas de COGESS, por exemplo, são considerados dados sensíveis perante a LGPD. Se vazados, configurarão violação de intimidade das pessoas atingidas, com consequências legais desastrosas para a SEGES, na forma de sanções diversas, afastamentos e exonerações de responsáveis, sem prejuízo de sanções legais em outras esferas.

O prejuízo à credibilidade da SEGES também será severo, e levará tempo para a recuperação dessa mesma credibilidade. Na Matriz de Riscos acima, tal risco é considerado Risco Extremo, e que pede medidas severas para evitar que aconteça, bem como para estancar rapidamente as consequências, na infelicidade de o evento acontecer.

Formas de Prevenção:

- Sistemas de informação e bases de dados que contenham dados confidenciais e/ou sensíveis devem ter acesso restrito somente a quem de fato precisa de acesso a eles;
- Política de privilégios mínimos de acesso – cada usuário só dispõe das permissões mínimas necessárias para a execução de suas atividades; cancelamento de acesso dos usuários sempre que tais acessos deixem de ser necessários ou que os usuários deixem a Secretaria;
- Bases de dados pessoais sensíveis ou dados confidenciais devem estar em locais seguros, tanto fisicamente quanto virtualmente;
- Exigência de conexões seguras para acesso a tais sistemas e bases de dados;
- Logs nos sistemas de informação e trilhas de auditoria, para detecção e gravação de todas as ações de cada usuário;
- Prevenção de logins não-autorizados na rede corporativa;
- Recomenda-se que redes ou sistemas de informação que lidam com dados sensíveis deveriam dispor de “alertas” ou “gatilhos” sempre que uma operação crítica for tentada, evitando erros acidentais;
- Orientar usuários a jamais deixar dados sensíveis em suas estações de trabalho, sejam pessoais ou de posse da Secretaria. Idem para mídias externas como HDs, SSDs externos, pen-drives, blocos de papel, etc.

Forma de Tratamento: O tratamento do evento, em caso de materialização, será coberto no Manual do Plano de Continuidade de Negócios, pela gravidade de que um tal evento se reveste.

6.3 Quedas da internet

Evento com probabilidade média de ocorrência em SEGES, geralmente à razão de 1 ou 2 eventos por mês, em média. As ocorrências de queda ocasionam paralisação parcial a total das atividades em SEGES, a depender especificamente da área ou coordenadoria afetada, e esse impacto será tanto quanto maior for o tempo em que a internet estiver fora do ar, e também de quais áreas foram mais atingidas. Ou seja, é uma ocorrência com impacto de moderado a alto – dependendo da duração da interrupção - e de ocorrência com probabilidade média. Na Matriz de Riscos que montamos acima, tais combinações de impacto e probabilidade configuram um Risco Alto, que pede providências para prevenção e também para mitigação em caso de ocorrência.

Formas de Prevenção:

- Exigência de SLAs rigorosos para serviços de Redes e Conectividade, se possível;
- Canal extra de acesso à Internet, de operadora distinta do canal principal, se possível, e pronto para entrar em cena tão logo se verifique a queda do principal.

Formas de Tratamento: Geralmente, abre-se chamado junto ao provedor de acesso. Para maiores detalhes e para procedimentos adicionais, consultar o Manual do Plano de Continuidade de Negócios.

6.4 Quedas de energia elétrica

Evento com baixa ou muito baixa probabilidade de ocorrência em SEGES, porém com impacto imediato, na forma de paralisação total ou quase total das atividades. A intensidade esse impacto dependerá, como no caso da internet fora do ar, da duração da queda e das áreas que foram mais afetadas, podendo ir de impacto baixo – na queda por poucos minutos – a alto, se durar várias horas. Pela nossa Matriz de Riscos acima, o risco varia de Risco Baixo a Risco Moderado, e manda o bom senso que consideremos o risco real como Moderado, a fim de estarmos preparados para qualquer eventualidade.

Formas de Prevenção: Aqui, trata-se de prevenir não o evento de queda de energia, que pode ser ocasionado por fatores fora de nosso controle, mas prevenir algumas de suas consequências. Trata-se de promover uma cultura de backups frequentes de documentos e trabalhos importantes entre os colaboradores, para trabalho offline ou para pronta recuperação dos dados assim que a energia retornar.

Formas de Tratamento:

- Usar geradores e No-Breaks para alimentar máquinas tipo server que armazenam sistemas de informação, a fim de que estes não deixem completamente de operar ou que possibilite um tempo extra para o correto desligamento dos equipamentos.
- Manter operacionais switches, roteadores, máquinas tipo client (todas ou somente uma parte delas, por um tempo determinado), reduzindo o impacto da queda de energia, até que a mesma seja restabelecida;

No caso específico da SEGES, tais medidas dependem de fatores fora de nosso controle, de modo que ficam apenas como sugestões.

6.5 Acesso não autorizado à rede corporativa e a sistemas de informação

Este evento pode ser considerado como tendo probabilidade de baixa a média, e suas consequências podem variar grandemente, a depender do que efetivamente foi acessado. O risco maior é o acesso a informações sensíveis, o que pode render consequências muito desagradáveis. Portanto, podemos considerar este Risco como sendo Alto ou Extremo e, portanto, deve ser evitado a todo custo.

Formas de Prevenção:

- Concessão de acesso à rede corporativa e a sistemas de informação limitados somente aos usuários que necessitam de tal acesso;
- Limitar as permissões de acesso à rede e aos sistemas de informação às funcionalidades mínimas necessárias para a realização das atividades pretendidas;

- Revogar o acesso dos usuários à rede e aos sistemas de informação, quando tal acesso não for mais necessário ou quando o usuário deixar a Secretaria;
- Tanto a rede quanto os sistemas de informação deverão impedir acessos concorrentes com o mesmo usuário, e sempre registrar – em logs ou trilhas de auditoria – quando tais acessos ocorreram, e por qual usuário;
- Instruir os usuários a jamais compartilharem seus logins e senhas de acesso, especialmente com pessoas externas à Secretaria.

Formas de Tratamento: Para medidas de tratamento, consultar o Manual do Plano de Continuidade de Negócios.

6.6 Vandalismo e roubo de equipamentos

Probabilidade relativamente baixa de ocorrência em SEGES. Porém precisamos lembrar que suas consequências podem ser potencialmente danosas, indo desde a perda de trabalhos de um determinado servidor da Secretaria até o acesso a bases de dados confidenciais ou a sistemas de informação com acesso restrito. Para não citar o óbvio, que é o prejuízo financeiro com a perda, quebra ou vandalização do equipamento em si. Ou seja, o impacto pode variar de Moderado a Muito Alto, a depender dos ativos que foram alvo do ataque físico. Esta combinação de impacto e probabilidade acarreta um Risco que varia entre Moderado e Alto, e que a prudência recomenda considerar como Alto.

Formas de Prevenção:

- Controle de acesso físico aos ativos de TIC da Secretaria – isto pode não depender só da SEGES, a depender dos locais onde os ativos estão e de como podem ser fisicamente acessados;
- Contratação de algum tipo de seguro para os equipamentos de TIC (transferência de riscos financeiros)
- Orientar colaboradores a evitar deixar arquivos, informações sensíveis, bases de dados – sejam estes dados sensíveis ou não - em suas estações de trabalho, utilizando sempre recursos ofertados pela Secretaria para o propósito de guarda de documentos digitais e bases de dados. Esta medida pode não prevenir o incidente em si, mas diminui seu impacto.

Formas de Tratamento:

- Comunicação imediata do furto/roubo/vandalismo/desaparecimento do ativo de TIC à área competente – CAF- no caso de realmente acontecer o evento indesejado, bem como efetuar o boletim de ocorrência (BO).

6.7 Perdas de código-fonte de soluções desenvolvidas internamente

Situação desagradável que pode acontecer em virtude de ataque externo (hacker) ou de dano – por qualquer motivo - a máquina onde estejam armazenados os códigos-fontes, eventuais bases de dados, APIs, etc., que tenham sido desenvolvidos internamente.

Este é um risco com impacto que classificaríamos de Alto. E com probabilidade de baixa a média de ocorrência, o que, pela nossa Matriz de Risco, representa um risco Alto.

Formas de Prevenção:

- Limitação do acesso ao código-fonte dos programas desenvolvidos internamente aos respectivos desenvolvedores e seus supervisores;
- Recomenda-se fazer backups periódicos de tais códigos-fonte e mesmo de bases de dados a eles associadas, seja em outra máquina física, seja na nuvem;
- Recomenda-se ainda confirmar se os backups mantém as vulnerabilidades dos códigos originais ou não, e checar se os backups estão sempre operacionais, isto é, em condições de uso caso precisem ser acionados.

Formas de Tratamento:

- Acionar os backups existentes;
- Apurar os motivos da perda e, onde cabível, apurar responsabilidades.

6.8 Indisponibilidade de um sistema de informação estruturante

A SEGES faz uso de uma série de sistemas de informação em suas atividades diárias, quais sejam o SEI, o SIGPEC, o SUPRI, o SIMPROC, o GESTÃO.NET, etc. Destes, os mais críticos para as atividades da Secretaria são o SEI, o SIGPEC e o SUPRI. E é nesses sistemas que focaremos nossa análise.

Em geral, as bases de dados, espaços de armazenamento, máquinas server e demais recursos de TIC associados a tais sistemas não estão nas dependências de SEGES, mas sim em órgãos como a PRODAM e similares.

Por melhores que sejam as práticas de segurança de TIC adotadas nas entidades que cuidam da sustentação dos referidos sistemas de informação, sempre há algum risco de que tais sistemas apresentem instabilidades, falhas em uma ou mais funcionalidades, indisponibilidade, necessidade de manutenção preventiva ou corretiva, dentre outros eventos potencialmente desagradáveis. Estamos desconsiderando aqui os problemas do acesso à rede corporativa e queda da rede, bem como os de queda de energia elétrica, que são problemas de infraestrutura e não de software.

Normalmente, em SEGES são abertos chamados junto às entidades que cuidam da sustentação de um dado sistema crítico, quando este apresenta falhas que comprometam seriamente ou impeçam sua utilização. O impacto de tal situação pode variar em função das funcionalidades afetadas, das áreas da SEGES que necessitam usar tal sistema, dentre outros fatores, mas vamos tomá-los por Altos ou Muito Altos, pelo impacto em processos de trabalho essenciais, como folha de pagamento, agendamento de perícias médicas, dentre outros.

A probabilidade de ocorrência, pelo nosso histórico, pode ser dada como baixa ou no máximo média, mesmo para sistemas críticos como os listados no parágrafo anterior. Pela Matriz de Riscos, o risco – para os sistemas críticos - pode ser considerado Alto.

Formas de Prevenção:

- Dispor de SLAs rigorosos com os responsáveis pelos datacenters que sustentam os sistemas de informação estruturantes;

- Fornecedores e/ou Datacenters alternativos, que entrem em cena tão logo ocorram falhas no Datacenter principal.

Formas de Tratamento: Inicialmente, pronta abertura e acompanhamento de chamado junto ao fornecedor. Para mais informações, consultar o Manual de Plano de Continuidade de Negócios, associado ao presente documento.

6.9 Vírus, Phishing e Malware

Riscos sempre presentes. Usuários podem clicar em e-mails e links suspeitos, que a seu turno podem abrir caminho para a instalação de malware em seus respectivos computadores pessoais ou de trabalho, acessando dados pessoais, roubando dados que deveriam estar protegidos, dentre outras consequências. Vírus podem apagar ou alterar conteúdo nas estações de trabalho e, em casos mais extremos, inutilizar as máquinas. Desta forma, podemos classificar o risco aqui como Extremo, tanto pela probabilidade elevada de ocorrência como pelo impacto potencial do problema, que pode vir a ser muito alto.

Formas de Prevenção:

- Antivírus sempre atualizado;
- Campanhas de esclarecimento para os colaboradores no sentido de não abrirem e-mails e links suspeitos, etc.

Formas de Tratamento:

- Consultar o Manual de Plano de Continuidade de Negócios.

6.10 Descartes inadequados de equipamentos antigos

Equipamentos antigos podem ter, especialmente nos seus respectivos HDs e SSDs, dados diversos. Estamos supondo aqui que dados sigilosos já haviam sido guardados na nuvem, e não no equipamento descartado, o que diminui consideravelmente os riscos para a SEGES caso o equipamento caia em mãos erradas após o descarte. Consideraremos o risco, assim, como Moderado.

Formas de Prevenção:

- Em SEGES, já temos a boa prática de fazer backup dos dados presentes em equipamentos antigos, para que possam ser transferidos para equipamentos mais novos.
- Além disso, dispomos de aplicativos que apagam todo o conteúdo de HDs e SSDs dos equipamentos que serão descartados, para garantir que não sobrem dados nesses espaços de armazenamento após o descarte.

6.11 Mais alguns tipos conhecidos de risco

- Wi-Fi mal protegido;
- Senhas fracas.

7. TRATAMENTO DE RISCOS

O tratamento de riscos, em essência, é a resposta planejada aos riscos encontrados. Envolve decidir se o risco vai ser tratado ou não, com base na priorização dos riscos realizada conforme a Matriz de Risco. A estratégia de tratamento de risco a ser adotada em SEGES é composta pelas opções: modificar o risco, aceitar o risco, evitar o risco e compartilhar o risco.

Com base em tais considerações, podemos montar uma tabela simples descrevendo tais opções de tratamento de risco, como demonstrado na tabela de Tratamento de Risco abaixo:

Tratamento de Risco

Opção de Tratamento	**Descrição**
Modificar	O risco precisa ser gerenciado pela inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e considerado aceitável.
Aceitar	O objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis. Em algumas situações, como: risco de baixo nível ou custo muito alto face ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco.
Evitar	Significa basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de uma divisão ou processo de trabalho.
Compartilhar	Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras.

Outro conceito que pode ajudar a gestão de riscos, é o de "limite de tolerância a riscos", abaixo do qual podem ser aceitos os riscos que lá constam, sem medidas de controle. Ou, quando muito, se os gestores de riscos de TI assim o desejarem, alguns desses riscos tomados como baixos podem ser mitigados com medidas bastante simples e baratas de implementar, especialmente quando não se deseja sobrecarregar equipes de suporte, como no caso já citado de esquecimento de senhas.

É razoável considerar esse limite de tolerância como a linha que, na Matriz de Risco, separa os riscos Moderado e Baixo. O que estiver do lado do Risco Baixo pode simplesmente ser aceito ou mitigado com medidas simples, como vimos. Um ponto que não pode ser esquecido, por ocasião da definição de medidas de tratamento de risco, é saber quem irá se responsabilizar pelas ações de tratamento.

7.1 Pequeno resumo de eventos, riscos e tratamentos

A tabela a seguir resume o que discutimos nas seções anteriores:

Evento	**Risco Inerente**	**Tratamento do Risco**	**Existe a medida de tratamento em SEGES?**	**Quem executa a medida?**
Esquecimento de senha	Baixo	Mecanismo de recuperação de senha fácil de usar e bem estabelecido	Acionamento ao Núcleo de Suporte	COTIC Núcleo Suporte
Perda de bases de dados	Extremo	Existência de backups operacionais das bases; Armazenamento seguro das bases e de seus backups; Controle severo de acesso às bases de dados	Existe política de backup seguindo Orientação Técnica do Orgão Central	COTIC Núcleo Suporte

Vazamento de dados sensíveis e/ou sigilosos	Extremo	Controle severo de acesso a bases de dados e sistemas de informação; Não deixar informações sensíveis à mostra, etc.	Aplicar passos determinados na Política de Segurança da Informação.	COTIC Núcleo Suporte
Queda da Internet	Alto	Redundância de links de acesso e de provedores	Acionamento da Prestadora de Serviços.	COTIC Núcleo Suporte
Queda de Força	Moderado	Hábito de fazer backups frequentes de documentos e trabalhos importantes; Uso de no-breaks e geradores;	Acionamento da área fiscalizadora da prestação de serviço.	CAF/DIAP
Acesso não autorizado à rede corporativa	Alto	Controle de acessos severo; Política de revisão periódica de privilégios e permissões de acesso; Cancelar acessos de pessoas que encerraram vínculos com a Secretaria; Exigir senhas consideradas “fortes”, etc	Há regras automatizadas de política de acesso à rede corporativa que efetua o bloqueio de acesso dos colaboradores.	COTIC Núcleo Suporte

Vandalismo e furto/roubo	Alto	Controles de acesso físico; Guardar equipamentos como notebooks, tablets e afins em local seguro. Fazer Boletim de Ocorrencia.	Contratação de segurança predial; Em caso de furto/roubo acionar CAF.	CAF
Perda de software desenvolvido localmente	Muito Alto	Antivírus atualizado, campanhas educativas para colaboradores.	Isolamento do equipamento da rede Corporativa e formatação do equipamento.	COTIC Núcleo Suporte
Senha Fraca	Alto	Instruir colaboradores para que criem senhas fortes, além de criarem o costume de trocá-las periodicamente e guardá-las em local seguro.	Política de senha ativa, impossibilitando senhas fracas. Comunicados orientativos aos usuários.	COTIC Núcleo Suporte
Paralisação de sistemas estruturantes	Alto	Pronta abertura e acompanhamento de chamados; Acesso a backups de bases de dados dos sistemas afetados; Redundância de servers e bases de dados na PRODAM	Abrir chamado técnico junto a prestadora de serviço e acompanhar status. Demais medidas competem à PRODAM.	COTIC Núcleo Suporte / COTIC Núcleo Contratos

Descarte Inadequado de Equipamentos	Moderado	Em SEGES, já temos a boa prática de fazer backup dos dados presentes em equipamentos antigos, para que possam ser transferidos para equipamentos mais novos. Além disso, dispomos de aplicativos que apagam todo o conteúdo de HDs e SSDs dos equipamentos que serão descartados, para garantir que não sobrem dados nesses espaços de armazenamento após o descarte.	SIM	COTIC Núcleo Suporte

7.2 Documentações sobre lições aprendidas

Um ponto importante é cuidar para que lições aprendidas com qualquer incidente sejam devidamente documentadas, tanto para servirem de referência sobre como agir em situações semelhantes, quanto para apoiarem e mesmo melhorarem a gestão de riscos.

8. RISCO RESIDUAL

O risco que permanece, após as medidas de tratamento terem sido tomadas, é chamado risco residual, em contraposição ao risco pré-tratamento, chamado também de risco inerente, do qual já falamos neste documento.

No que toca aos controles e medidas de tratamento para a gestão do risco, temos a tabela abaixo:

CLASSIFICAÇÃO DO NÍVEL DE CONTROLE / MEDIDAS DE TRATAMENTO

Nível do Controle	**Descrição**
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.
Fraco	Os controles existentes têm abordagens ad hoc, ou seja, tendem a ser aplicados caso a caso, e a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.
Médio	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.

Seguindo as recomendações da Controladoria Geral da União (CGU), o cálculo do nível de risco deve ser realizado pensado em dois cenários distintos:

1. Risco inerente – imaginar o processo em questão sem nenhum mecanismo de controle implementado - é o risco que discutimos nas seções anteriores.

2. Risco residual – imaginar o processo em questão com os atuais mecanismos de controle implementados.

A diferença entre o risco inerente e o risco residual demonstrará a atual eficácia dos controles implementados na mitigação dos riscos identificados. A partir das orientações acima, poder-se-ão, oportunamente, avaliar os controles internos referentes aos riscos de TIC encontrados em SEGES.

Uma medida de riscos residuais pode ser quantitativa ou qualitativa, e dependerá de como foi feita a classificação de riscos inerentes. Se esta última foi quantitativa, a medida dos residuais será também quantitativa. Se foi qualitativa, os riscos residuais também serão avaliados qualitativamente.

Como fizemos a avaliação dos riscos inerentes de modo qualitativo, a dos riscos residuais, por coerência, também será assim.

O raciocínio aqui proposto é simples:

- Um Risco Inerente Extremo, se submetido a um Controle Forte, poderá virar um Risco Residual Baixo; se submetido a um Controle Satisfatório, poderá ser reduzido a um Risco Residual Baixo ou Médio. Um controle Mediano o levará a um Risco Residual Alto ou Médio; controles Fracos o levarão a Riscos Residuais Altos ou Extremos, e controles Inexistentes manterão o Risco Residual no nível Extremo.

- Um Risco Inerente Alto, submetido a um Controle Forte ou Satisfatório, poderá ser reduzido a um Risco Residual Baixo. Um controle Mediano o levará a um Risco Residual Médio, e controles Fracos ou Inexistentes manterão o Risco Residual no nível Alto.

- Um Risco Inerente Médio, se submetido a um Controle Forte, Satisfatório ou até mesmo Mediano, poderá virar um Risco Baixo. Mas poderá se manter em Risco Residual Médio se o Controle for Fraco ou Inexistente.
- Um Risco Inerente Baixo, com qualquer nível de Controle, ou mesmo sem Controles, permanecerá como Risco Residual Baixo.

Desta forma, o Risco Residual será sempre menor ou igual ao Risco Inerente original, jamais maior.

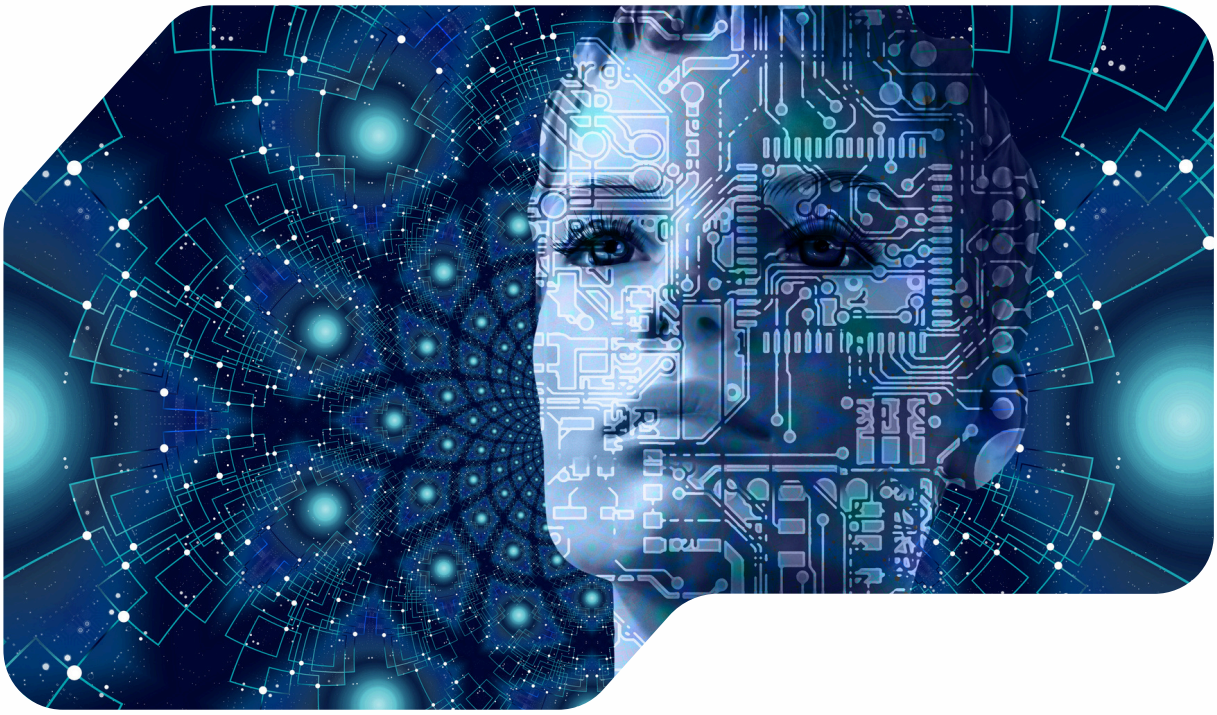
Qualitativamente, podemos montar uma Matriz de Risco Residual, a partir dos Riscos Inerentes e dos Controles. Uma proposta de matriz é como segue:

MATRIZ DE RISCO RESIDUAL, PARTINDO DE RISCO INERENTE E CONTROLE

Risco Inerente/ Controle	**BAIXO**	**MÉDIO**	**ALTO**	**EXTREMO**
Inexistente	BAIXO	MÉDIO	ALTO	EXTREMO
Fraco	BAIXO	MÉDIO	ALTO	ALTO/EXTREMO
Mediano	BAIXO	BAIXO	MÉDIO	MÉDIO/ALTO
Satisfatório	BAIXO	BAIXO	BAIXO	BAIXO/MÉDIO
Forte	BAIXO	BAIXO	BAIXO	BAIXO

A utilidade desta matriz é justamente apoiar o monitoramento dos riscos, tarefa essencial na Gestão dos Riscos e, tal como se passa com outras matrizes e tabelas deste material, poderá ser revisada e atualizada sempre que necessário.

Poderemos, em momento oportuno, avaliar os controles e medidas de mitigação que já temos e que discutimos na seção 07 acima, a fim de determinarmos os riscos residuais a partir dos riscos inerentes já mapeados. Em outras palavras, podemos pensar no risco residual como uma medida da eficácia dos controles e medidas de mitigação, bem como de monitoramento dos riscos como um todo, o que nos leva à próxima e última seção deste Manual.



9. MONITORAMENTO - POSSÍVEIS MÉTRICAS AUXILIARES DA GESTÃO DE RISCO

Monitorar os riscos e mesmo os controles de risco é tarefa essencial de qualquer boa gestão de risco.

Na seção anterior propusemos uma classificação de controles quanto à sua força (eficácia) e também como esses controles levam os riscos inerentes em riscos residuais. Mas há outras possibilidades de monitoramento de riscos, como os Indicadores-Chave de Risco.

Indicadores-Chaves de Risco em TI, em inglês KRIs (Key Risk Indicators), são métricas que auxiliam na gestão de riscos, indicando se tal gestão está funcionando a contento ou se precisa de atualizações e mudanças. Indicadores de risco necessitam de acompanhamento regular.

Ou seja, esses riscos podem ser prejuízos financeiros, fraudes, gaps de informação, falhas de segurança, técnicas ou logísticas, irregularidades legais, tendências e mudanças no mercado ou contexto social (crises econômicas, pandemias mundiais), entre outras coisas.

Para a área de TI, um rol sugestivo de KRIs é dado na tabela Indicadora de Riscos abaixo.

Tabela de Indicadores-Chave de Risco Sugeridos para Acompanhamento

Risco	**KRI**	**Motivo para acompanhar o risco**
Falha no Provedor de Serviços de Internet (I)	Número de vezes em que ficamos sem Internet	Atividades em SEGES podem parar quase que por completo sem a Internet. Se houver muitas quedas de rede, melhor seria trocar de provedor.
Falha no Provedor de Serviços de Internet (II)	Tempo total (em minutos ou horas) por Mês sem internet	Idem
Perda de dados	Número de vezes em que backups de sistemas falharam	Updates em softwares podem causar falhas em backups
Incidentes críticos sem solução (I)	Tempo médio que se leva para resolver um incidente crítico	Se o tempo de resposta a incidentes críticos for alto, então precisamos mudar os procedimentos de resposta a incidentes críticos na SEGES
Incidentes críticos sem solução (II)	Número de incidentes críticos sem solução	Muitos incidentes críticos sem solução podem indicar falhas de projeto em sistemas de informação ou gargalos graves na infraestrutura.

Vazamentos anônimos de dados	Número de usuários administradores de bases de dados que estão ativos	Se há contas de administradores “default”, fica difícil saber quem é o responsável por um vazamento de dados.
Arranjos de segurança impróprios	Número de usuários com funções semelhantes, mas com arranjos de segurança divergentes	Usuários podem estar acessando bases de dados em SEGES que não deveriam estar acessando.
Malware	Número de usuários que clicam em links suspeitos em e-mails e sites diversos.	Testar usuários com e-mails de phishing falsos serviria para saber quem precisa de treinamento ou dicas extras de segurança. Os que clicassem no link falso de e-mail precisariam de reforço nas orientações de segurança.
Interrupção no serviço de um fornecedor	Número de fornecedores sem SLA	Fornecedores sem um SLA com a SEGES podem ser um problema, pois não ficam contratualmente obrigados a atender aos nossos padrões de qualidade. Tal situação pode levar a serviços mal executados e, no limite, interromper rotinas importantes em SEGES.
Descumprimento de dispositivos da LGPD	Tempo para responder a requisições sobre dados pessoais	Riscos legais e mesmo financeiros envolvidos.

Credenciais de acesso compartilhadas (I)	Número de sistemas concorrentes usando o mesmo acesso (login)	Pode indicar que há usuários compartilhando suas credenciais com indivíduos não-autorizados.
Credenciais de acesso compartilhadas (II)	Número de vezes em que há sistemas concorrentes usando o mesmo login em um dado período (ex: em uma semana, em um mês)	Verificar com que frequência está ocorrendo o possível compartilhamento de credenciais com pessoas não-autorizadas.
Falta de compliance	Frequência com a qual os direitos de acesso privilegiado em sistemas de TIC são revisados	Essas contas com acessos privilegiados podem ser alvo da ação de hackers, que poderão usá-las para acessar dados sensíveis ou críticos da SEGES.

Recomenda-se que alguns dos KRIs indicados acima sejam adotados e monitorados periodicamente em SEGES, com a definição de quais KRIs serão efetivamente acompanhados vindo em momento oportuno.

PREFEITURA DE
SÃO PAULO