PROGRAMA DE SEGURANÇA DA INFORMAÇÃO E GOVERNANÇA EM PRIVACIDADE

Este documento transcreve os objetivos traçados para obter a Governança em Privacidade do Poder Executivo Municipal, nos termos do art. 50 da LGPD[U17] , terá como objetivo a adequação aos requisitos da LGPD, dispondo de um conjunto de atividades que serão traduzidas em ações concretas a serem atingidas, considerando ainda a estrutura organizacional do Município de Rio dos Cedros, de forma a construir uma lista de atividades que se adeque à realidade deste ente.

Rio dos Cedros-SC
2023

Sumário

PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

Apresentação

Considerando que os dados podem ser usados na tomada de decisões importantes, seu valor é reconhecido e deve ser preservado. O grande valor atrai grandes ameaças. Não devem cair nas mãos erradas. Adulterações e indisponibilidade podem levar a decisões erradas ou falta de ação.

Estas são as bases e justificativas para a Segurança da Informação, que visa a manutenção da Confidencialidade, Integridade e Disponibilidade das informações. E o instrumento importante para isso é a Política de Segurança da Informação, um conjunto de diretrizes, normas, procedimentos e padrões a serem observados e seguidos por todas as pessoas que utilizarem a infraestrutura do município.

Diretrizes

Estes são os princípios básicos que regem a Política de Segurança, estabelecidos de acordo com as necessidades da instituição.

1. À Administração do município de Rio dos Cedros é atribuída a guarda de informações de seus munícipes, fornecedores e empregados. Portanto, a criação de um ambiente que garanta a disponibilidade e proteção é essencial para a continuidade das políticas públicas.
2. Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade, integridade e disponibilidade e ser tratada de acordo com a sua classificação, independente da sua forma de armazenamento, digital ou não.
3. Dados Pessoais e informações relacionadas a pessoa natural identificada ou identificável, devem obrigatoriamente ser protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD) e tratados como confidenciais quando não houver justificativa legitima em contrário. Cuidados redobrados devem ser tomados em relação aos Dados Pessoais Sensíveis, aqueles que podem revelar origem racial, étnica, opinião política, convicção religiosa, filosófica, filiação sindical, dados genéticos ou biométricos, relacionados a saúde, vida sexual ou orientação sexual.
4. As informações devem ter o ciclo de vida programado. Informações consideradas confidenciais, quando não mais necessárias, devem ser destruídas através de mecanismos apropriados. O descarte ou reutilização de mídias contendo essas informações deve ser feito de forma a inviabilizar a recuperação das mesmas.
5. Todo o indivíduo que tenha acesso a dependência deverá ser identificado. O acesso de terceiros em áreas onde exista o processamento físico ou digital de informações deverá ser fundamentado pela estrita necessidade e deverá ocorrer sempre com o acompanhamento de empregado da Administração Municipal, responsável pelas informações naquele setor.
6. Todos os equipamentos na administração municipal deverão estar inventariados e identificados de forma individual.
7. Credenciais de acesso as instalações e sistemas são pessoais, não compartilháveis e intransferíveis. O usuário é responsável por todas as atividades desenvolvidas mediante autenticação com sua credencial, por isso deve zelar por sua proteção e sigilo, e realizar as ações de manutenção apropriadas para cada tipo de credencial, como a troca periódica de senhas.
8. Alterações no ambiente de produção devem ser previamente estudadas, formalizadas por processo padronizado, comunicadas, autorizadas e, sempre que possível, testadas em ambiente apropriado e isolado, anteriormente à efetiva colocação dos recursos em produção, para verificação e avaliação dos impactos causados no processo produtivo, com o objetivo de garantir a estabilidade do ambiente.

9. Os empregados, durante a vigência e após o término do contrato de trabalho ou prestação de serviço, não podem se apropriar de informações ou de mídias, equipamentos, componentes ou acessórios que as contém, como por exemplo: e-mails corporativos, planilhas, arquivos de dados ou vídeos.
10. A responsabilidade de manter a segurança é compartilhada por todos os funcionários. A Administração Municipal deverá ministrar treinamentos para promover a conscientização e preparo.

Normas

Violações das normas abaixo relacionadas, incidentes ou falhas de segurança devem ser notificadas imediatamente à equipe de Tecnologia de Informação da Prefeitura Municipal de Rio dos Cedros – SC.

Se houver mera possibilidade de vazamento de Dados Pessoais, deve ser notificado também imediatamente o Encarregado de Processamento de Dados (DPO).

Segurança Física

1. Todo o indivíduo ao ingressar nas instalações da Administração deverá usar crachá de identificação.
2. Pessoas externas à Administração Municipal deverão ser identificadas nas recepções dos prédios da administração municipal e o seu ingresso nas instalações será realizado mediante autorização e acompanhamento de colaborador do município.
3. Todo o equipamento que ingressar ou sair da administração municipal, deverá estar acompanhado da respectivo registro e autorização do setor de Patrimônio.
4. Os prestadores de serviços da Administração Municipal são responsáveis pelas ações ou prejuízos causados por seus empregados ao patrimônio, bem como deverão garantir a manutenção da confidencialidade das informações acessadas.
5. Documentos ou papeis contendo informações confidenciais, quando não mais necessários, devem ser triturados ou destruídos de forma a impossibilitar leitura.
6. Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc) contendo informações confidenciais, quando não mais necessárias, devem ser quebradas ou destruídas de forma a impedir seu uso indevido.
7. Mídias regraváveis (drives HD ou SSD, pen drives, cartões SD, fitas, discos CD ou DVD do tipo RW, ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas com o procedimento seguro adequado indicado pela equipe de Segurança da Informação antes de seu reuso ou descarte.
8. A entrega de documentos com informações confidenciais pode ocorrer apenas com registro e a garantia de identificação de quem recebe e mediante prévia assinatura de termo de confidencialidade.
9. Os equipamentos e seus componentes internos serão inventariados periodicamente e somente funcionários autorizados podem fazer remanejo de equipamentos e peças.

Credenciais

1. Credenciais, identificações e senhas de acesso devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.
2. Cada funcionário deve trocar periodicamente suas senhas e é de sua responsabilidade escolher senhas robustas, complexas e longas.
3. As senhas devem ser únicas, não devem ser usadas senhas idênticas ou semelhantes para identificação em sistemas, sites ou serviços não gerenciados pelos Gestores de Sistemas da Administração Municipal, sejam de natureza pessoal ou não.

Uso da Rede

1. O acesso a Internet é fornecido para atividades e finalidades da Administração Municipal. Acessos com fins particulares lícitos podem ser feitos ocasionalmente, preferencialmente fora do horário de expediente, desde que não violem as demais normas.
2. É proibido usar a rede para acessar ou enviar conteúdo pornográfico, ofensivo ou difamatório, bem como para constranger terceiros, sejam eles funcionários ou não.
3. O uso para fins particulares de redes sociais como Facebook ou Twitter e sítios de vídeos como YouTube, Vimeo e Netflix durante o horário de expediente é considerado inadequado e pode estar bloqueado a qualquer horário a critério da Administração Municipal.
4. Qualquer sítio conhecido de conteúdo vedado ou inadequado pode estar em listas de bloqueio automático. Eventuais erros na classificação de determinado sítio podem ser comunicados à equipe responsável pelos proxys para retificação.
5. Os acessos à Internet podem ser monitorados e registrados pela Administração Municipal. Os registros ficam a disposição da Administração Municipal pelo tempo que esta julgar adequado.
6. O compartilhamento de recursos nas estações de trabalho deve ser limitado a atividades de interesse da Administração Municipal, com liberação somente para leitura por conjunto restrito de usuários.
7. Não é permitido instalar, usar ou configurar equipamentos (hardware ou software) que deem acesso à rede corporativa sem autorização formal e conhecimento da Equipe de Segurança da Informação. Em especial, não é permitida a instalação de ponto de acesso wifi, bluetooth, modem, hub, switch, vpn, roteador ou software de acesso remoto para fins pessoais.
8. Não é permitido copiar arquivos ou realizar acessos com fins particulares que onerem excessivamente a utilização da rede.
9. Todas as mensagens enviadas por correio eletrônico com o endereço profissional são de propriedade da Administração Municipal, portanto devem ser usadas para assuntos de interesse da mesma e não se deve manter qualquer expectativa de privacidade de seus conteúdos.
10. É vedado o envio ou participação em correntes, mesmo de solidariedade, premiações ou informações.
11. É vedado o envio de mensagens com conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política.

12. Não é permitido distribuir, via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo “corrente” e mensagens em massa, comerciais, de propaganda política ou o envio de correio eletrônico não solicitado, SPAM.
13. Notebooks, laptops, tablets e outros equipamentos pessoais ou de terceiros não devem ser ligados diretamente na rede da Administração Municipal sem autorização. Tais equipamentos podem ser conectados à rede wifi e ter acesso a serviços internos via VPN gerenciada pela Administração Municipal.

Proteção de Estações

1. Em todas as estações de trabalho, notebooks e laptops deve estar instalado, ativo e atualizado o antivírus corporativo indicado pela equipe de administração do antivírus para o seu sistema operacional.
2. O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da equipe de administração do antivírus.
3. Constatado qualquer problema com o antivírus, o usuário deverá comunicar aos responsáveis pela administração do antivírus que tomarão as providências cabíveis.

Utilização de Programas

1. As estações de trabalho são disponibilizadas com os programas - sistema operacional e aplicativos - mínimos necessários para o desempenho de sua função básica.
2. São considerados legítimos os softwares instalados e utilizados conforme suas licenças de uso e que não contrariem as demais regras da Administração Municipal e a legislação. Em especial, esta norma contempla a possibilidade de uso de software livre para fins legítimos e não abusivos.
3. Não é permitida a instalação nos equipamentos da Administração Municipal de qualquer software, gratuito ou não, sem as devidas licenças para uso comercial da Administração Municipal.
4. O uso ou instalação de software sem licença de uso ou em nome de outros sem autorização caracteriza crime de pirataria, ficando o usuário e o instalador sujeitos às sanções administrativas, legais e penais da legislação.
5. Ocasionalmente serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software permitindo identificar desvios das normas.

Cópias de Segurança ou Backup

1. Cada usuário é responsável pela manutenção de cópias de segurança de seus arquivos de dados.
2. Arquivos gerados nas estações de trabalho que necessitem cópia de segurança deverão ser armazenados em servidor de arquivos apropriado da Administração Municipal, desde que autorizado pelo supervisor. É responsabilidade do funcionário confirmar com a equipe de Backups que as pastas estão incluídas nas rotinas de cópias de segurança.
3. Não é permitida a cópia de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não autorizados pela Administração Municipal ou cliente.
4. Sempre que possível, os dados confidenciais devem estar criptografados nos backups.
5. O responsável pelo servidor deverá ativar o processo de backup das informações críticas, incluindo serviços como correio eletrônico, banco de dados e aplicações.
6. Todo o backup deve periodicamente passar por teste de restauração.
7. Meios de armazenamento devem ser guardados em local seguro, armário, cofre ou sala com chave ou controle de acesso e devem ser respeitados os tempos de vida útil sugeridos pelo fabricante.
8. Alguns backups têm tempo de vida determinado por lei, portanto a equipe responsável pelos backups deve ser informada e zelar por mantê-los disponíveis durante esse tempo, bem como os equipamentos necessários para sua recuperação quando necessário.

Sistemas e Aplicações

1. Não é permitida a transferência de dados para processamento ou armazenamento em serviços externos, de terceiros não autorizados expressamente pela Administração Municipal ou cliente.
2. Armazenamento e transferências de dados confidenciais devem ser sempre criptografadas com mecanismos aprovados pela Administração Municipal.
3. Os sistemas devem gerar registros (logs) de eventos de segurança. Devem ser utilizados para este fim funções do Sistema de Segurança em uso, recursos do sistema operacional, recursos de banco de dados e/ou recursos da aplicação. Os registros devem conter ao menos as seguintes informações: identificação da aplicação e função, momento da ocorrência (timestamp), informações que identifiquem a máquina ou local da ocorrência e os dados relevantes manipulados pela aplicação. O Sistema de Segurança poderá se encarregar do registro de algumas dessas informações. Informações confidenciais não devem ser registradas em log sem estarem criptografadas.
4. No desenvolvimento e manutenção de sistemas é obrigatório o uso de software e repositório de controle e versionamento de arquivos (como fontes, modelos, documentos, diagramas, páginas web) aprovado pela Administração Municipal.
5. Cada desenvolvedor é responsável pela integridade dos arquivos de sistema que estão sendo trabalhados, devendo utilizar preferencialmente áreas de trabalho em servidores designados. Caso estejam residentes em sua máquina, o desenvolvedor deve providenciar cópia de segurança (backup) dos mesmos, quando necessária.
6. Todo o desenvolvedor de aplicações deverá seguir, quando disponíveis e forem aplicáveis, as recomendações de segurança para o desenvolvimento.

Administração de Servidores

1. Todas as instalações de novos servidores deverão seguir procedimentos padrões e incluir pacotes, Service Packs, Hot Fixes obrigatórios.
2. Após sua instalação o responsável deverá encaminhar à Equipe de Segurança solicitação para verificação complementar do servidor.
3. A instalação das atualizações de segurança deverá ser realizada pelo responsável direto de cada servidor, seguindo as orientações de segurança no que tange ao backup antes do procedimento, adequação de horário e plano de recuperação de falhas;
4. Acessos remotos devem ser feitos sempre usando mecanismos criptografados. Devem ser desativados os serviços de acesso remoto que não usam criptografia, tais como TELNET, FTP e VNCSERVER;
5. Os equipamentos utilizados devem possuir sistema operacional atualizado e com recursos de segurança.
6. A ativação de novos serviços de rede será condicionada a uma análise de riscos (a ser realizada pela Equipe de Segurança), onde, no mínimo, os seguintes aspectos serão considerados: requisitos de segurança do serviço, objetivo, alvo do serviço, forma de acesso, forma da administração e volume de tráfego.
7. Não é permitida a instalação de serviços de rede não autorizados pela Equipe de Segurança.

8. Todo o tráfego de informações confidenciais por meio compartilhado será protegido através de criptografia.
9. Sistemas de proteção de acesso (firewall) devem ser utilizados para permitir apenas às redes ou máquinas alvo dos serviços o acesso aos mesmos mediante solicitação para a equipe de Segurança.
10. A equipe de Segurança da Informação pode indicar e usar ferramentas de detecção e prevenção de intrusos, para emitir alertas e registrar possíveis tentativas de invasão.

Registros e Auditoria

1. Os administradores devem habilitar registros de segurança (logs), de forma a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditorias;
2. Os registros de segurança deverão ser analisados periodicamente (manual ou automaticamente).

Documentação Exigida

1. É fortemente recomendado que sistemas críticos tenham documentado o Plano de Continuidade de Negócio ou Recuperação de Desastre.
2. Todas as instalações e atualizações deverão ser documentadas pelo responsável, administrador ou desenvolvedor, inclusive:
    - Procedimentos para instalação;
    - Correções instaladas (service packs, hot fixes, patches);
    - Softwares instalados/atualizados;
    - Configurações a serem realizadas;
    - Permissões de acesso;
    - Contatos para suporte;
    - Informações Complementares.

Segurança Física de Servidores

1. O acesso físico aos servidores e equipamentos de infraestrutura deve ser restrito aos empregados e terceiros autorizados.
2. Os servidores e equipamentos de infraestrutura devem operar em ambiente adequado, s
3. Observar condições (temperatura, nível de poeira, umidade, etc) indicadas pelo fabricante.

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

APRESENTAÇÃO

O Programa de Governança em Privacidade regulamenta como é feito o tratamento de dados pessoais no âmbito do município de Rio dos Cedros e dá ênfase aos direitos e garantias dos titulares de dados de forma transparente.
Em cumprimento da Lei Geral de Proteção de Dados - LGPD, e com a preocupação constante de transparência e imparcialidade, ficam implementadas as novas práticas de segurança e os novos procedimentos de proteção a dados pessoais, com o objetivo de garantir a continuidade do interesse público nas áreas de privacidade dos cidadãos.
Com o propósito de satisfação dos seus clientes, fornecedores e empregados, enquanto Responsável pelo Tratamento dos seus Dados:

- Assegura que o tratamento dos seus Dados Pessoais é efetuado no âmbito da (s) finalidade (s), ou para finalidade (s) compatível (is) com o (s) propósito (s) inicial (is) para que foram coletados.
- Assume o compromisso de implementar uma cultura de minimização de dados, em que apenas se coleta, utiliza e conserva os dados pessoais estritamente necessários ao desenvolvimento das suas atividades.
- Não realiza a divulgação ou o compartilhamento dos dados pessoais coletados, para fins comerciais ou de publicidade.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) estabelece regras para o tratamento de dados pessoais com o objetivo de garantir a privacidade de cada um. A partir disso, a Coordenação de Processamento de Dados atualizou e criou políticas para continuar garantindo esses direitos.

Para complementar essa segurança, outras ações também foram tomadas: desde agosto de 2018, todos os novos contratos, com fornecedores e clientes, foram adequados à nova legislação; os contratos de trabalho dos profissionais foram aditivados para garantir que todos estejam cientes e comprometidos com as novas diretrizes; um firewall foi instalado, para ser mais uma camada de proteção dos servidores e dos acessos à internet feitos dentro da rede da Prefeitura.

A Prefeitura Municipal nomeou o encarregado pelo tratamento de dados pessoais através da portaria 324, de 03 de julho de 2022. (Thiago Richter Mastelotto - CPF 091.***.***-46

O conjunto de documentos a seguir é uma demonstração dos cuidados e compromissos da administração que está mantendo com os seus dados, em sua missão de operar tratamento de dados e dar assessoramento técnico para os órgãos da administração de nosso município.

Como a administração utiliza os dados pessoais coletados

Utiliza os dados pessoais para dar resposta aos seus pedidos, proceder à instrução dos seus processos, prestar informações sobre assuntos do seu interesse, para fins estatísticos e na realização de estudos de suporte à definição de políticas públicas municipais. Estes dados podem ser fornecidos através de requerimento, comunicação, participação e através dos canais de atendimento disponibilizados pela empresa: presencial, telefônico ou por via eletrônica.

Por fim, os dados pessoais poderão ser usados para: auditorias, análises estatísticas, ciência de dados e estudos para lançamento de novos serviços ou para a melhoria dos já existentes, bem como processos e comunicações. Nenhum dado pessoal poderá ser transferido ou compartilhado sem a prévia análise da conformidade com as bases legais previstas na LGPD.

Os dados pessoais que são coletados

Os dados pessoais coletados dependem do contexto das suas interações com a administração municipal e com a titular dos Dados Pessoais, no âmbito das atividades relacionadas e no cumprimento das atribuições que lhe estão legalmente cometidas.
Entre os dados coletados incluem-se os seguintes, não se limitando a eles:
Identificação: - Nome Completo; - Número do Registro Civil e do CPF; - Data de nascimento / idade. Contatos: - Endereço Residencial/Profissional; - Endereço de correio eletrônico/e-mail; - Número de telefone e/ou celular. Dados institucionais: Endereço de correio eletrônico /e-mail institucional. Dados Bancários e de Pagamento: no caso de solicitar algum serviço que implique pagamentos, ou no âmbito da execução de um contrato, coleta dos dados necessários para proceder ao processamento do respectivo pagamento, salário, reembolso.

Vídeo: se visitar instalações principalmente dos setores da Secretaria de Educação, a sua imagem pode ser captada pelas câmeras de segurança.

Voz: não armazenamos.

Digitais: são armazenados em banco de dados as digitais de nossos colaboradores, para fins de controle e fiscalização.

Da Coleta e Tratamento de Dados Pessoais de Menores

Os Dados Pessoais dos menores de idade, cuja coleta e tratamento não decorra de fundamento legal, somente serão coletados e tratados com o consentimento dos seus pais ou responsável legal. Os pais ou responsáveis legais têm a prerrogativa de exercer os direitos sobre os Dados Pessoais dos menores em condições similares aos dos titulares dos dados.

Da Coleta e Tratamento de Dados Sensíveis

Os Dados Pessoais de natureza sensível classificados na Lei Geral de Proteção de Dados (LGPD), em especial os que tratam sobre a origem racial ou étnica do seu titular, as suas opiniões políticas, as suas convicções religiosas, orientação sexual ou sobre a sua saúde (Dados Pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde e/ou que revelem informações sobre o seu estado de saúde), estão vinculados a um tratamento especial com salvaguardas técnicas e organizacionais específicas estabelecidas na LGPD.

Do Compartilhamento dos Dados

A administração municipal não repassará a terceiros, parceiros ou em qualquer negociação comercial, os dados pessoais coletados, exceto nas hipóteses de estrito cumprimento de obrigação legal, contrato, convênio ou instrumento congênere, determinação judicial ou mediante consentimento expresso destes.

Da Segurança de Dados Pessoais

Para segurança dos seus dados pessoais mantém uma equipe de profissionais qualificados e permanentemente atualizados nas melhores técnicas, utilizando um conjunto de tecnologias, ferramentas e procedimentos de segurança e desenvolvendo os melhores esforços para proteger os seus Dados Pessoais do acesso, uso ou divulgação não autorizados.

Do Controle dos Seus Dados Pessoais

A Administração Municipal, a seu pedido, garante o direito ao acesso, retificação, limitação de tratamento e eliminação dos seus Dados Pessoais, bem como, o direito de se opor ao seu processamento. Caso a utilização pela administração de seus dados pessoais seja baseada no consentimento, o titular tem o direito de o excluir, a qualquer tempo, sem comprometer a validade do tratamento de dados efetuado até o momento da solicitação formal da exclusão. O titular poderá, sempre que desejar, contatar o Encarregado pela Proteção de Dados contido no link Portal da Transparência - MUNICIPIO DE RIO DOS CEDROS (atende.net)) para esclarecer todas as questões relacionadas com o tratamento dos seus Dados Pessoais e exercício dos seus direitos enquanto titular de dados pessoais, bem como consultar informação sobre como exercer os seus direitos.

Como Posso Reclamar?

Por e-mail: ouvidoria@riodoscedros.sc.gov.br
Pela Web: Portal da Transparência - MUNICIPIO DE RIO DOS CEDROS (atende.net)
Por correspondência convencional:
A/C DPO OUVIDORIA; Rua Nereu Ramos, Centro, 205, Rio dos Cedros - SC – Brasil CEP 89121000. Sem prejuízo de poder apresentar reclamações diretamente ao setor de ouvidoria da administração municipal, caso assim o entenda, reclamar diretamente para a Autoridade Nacional de Proteção de Dados (ANPD).

Da Retenção de Dados Pessoais

A administração municipal, armazena os seus Dados Pessoais apenas pelo período de tempo necessário e no âmbito das finalidades para os quais os dados foram coletados, e conforme seja necessário para consecução de seus serviços. Os períodos de conservação dos seus dados podem mudar significativamente quando estejam em causa fins de arquivo de interesse público, científicos ou estatísticos, e compromete-se a adotar as medidas de conservação e segurança adequadas. Podendo vir a manter seus Dados Pessoais após receber seu pedido de exclusão ou após os prazos caso seja necessário para cumprimento de obrigações legais, resolver disputas, manter a segurança, evitar fraudes e abuso e garantir o cumprimento de contratos.

Dos Cookies e Tecnologias Semelhantes

A administração utiliza cookies para fornecer seus sites e serviços online ou ajudar a coletar dados e guardar as suas configurações, com o objetivo de melhorar o desempenho dos serviços da empresa e a sua experiência como usuário.

Das Alterações à Política de Privacidade

Esta política de privacidade será objeto de atualização permanente, de forma a refletir os comentários dos usuários e sempre que se justifique. Recomenda-se que ao titular do dado que verifique periodicamente a política de privacidade www.riodoscedros.sc.gov.br para se manter informado sobre como a administração está protegendo os seus Dados Pessoais e se manter atualizado sobre as informações e direitos que lhe assistem.

Princípios da política de mesas limpas e telas limpas

- Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancados, quando não estiverem em uso, especialmente fora do horário do expediente;
- Informações sensíveis ou críticas para o negócio da organização devem ser trancadas em local separado e seguro (um armário ou cofre à prova de fogo);
- Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;
- Não anotar informações sensíveis em quadros brancos;
- Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras;
- Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;
- Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;
- Fotocopiadoras devem ser protegidas contra uso não autorizado;
- Devolver, o quanto antes possível, todos os documentos obtidos por empréstimos de outros departamentos, quando eles não são mais necessários;
- Computadores pessoais e terminais de computador e impressoras não devem ser deixados “logados”, caso o usuário responsável não esteja presente;
- Nos computadores, utilizar um protetor de tela que solicite uma senha para acesso;
- Guardar agendas e cadernos de anotações numa gaveta trancada;
- Manter os pertences pessoais em gavetas ou armários trancados;
- Nunca deixar crachá de identificação ou chaves em qualquer lugar; mantenha-as junto a você;
- Notificar o pessoal da segurança imediatamente se seu crachá ou chaves sumirem;

- Nunca escrever senhas em lembretes e nem tente esconde-las no local de trabalho;
- Não deixe mídias, como CDs ou disquetes nos drives;
- Mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores;
- Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar computador;
- Manter as gavetas e armários fechados e trancados e não deixar as chaves na fechadura.
- Não colocar ou comer refeições e lanches sobre a mesa;
- Não colocar copos de água, suco, refrigerante ou café sobre a mesa;
- Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados;
- Trancar o local de trabalho ao deixá-la, não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA E PRIVACIDADE

Preparação Prévia

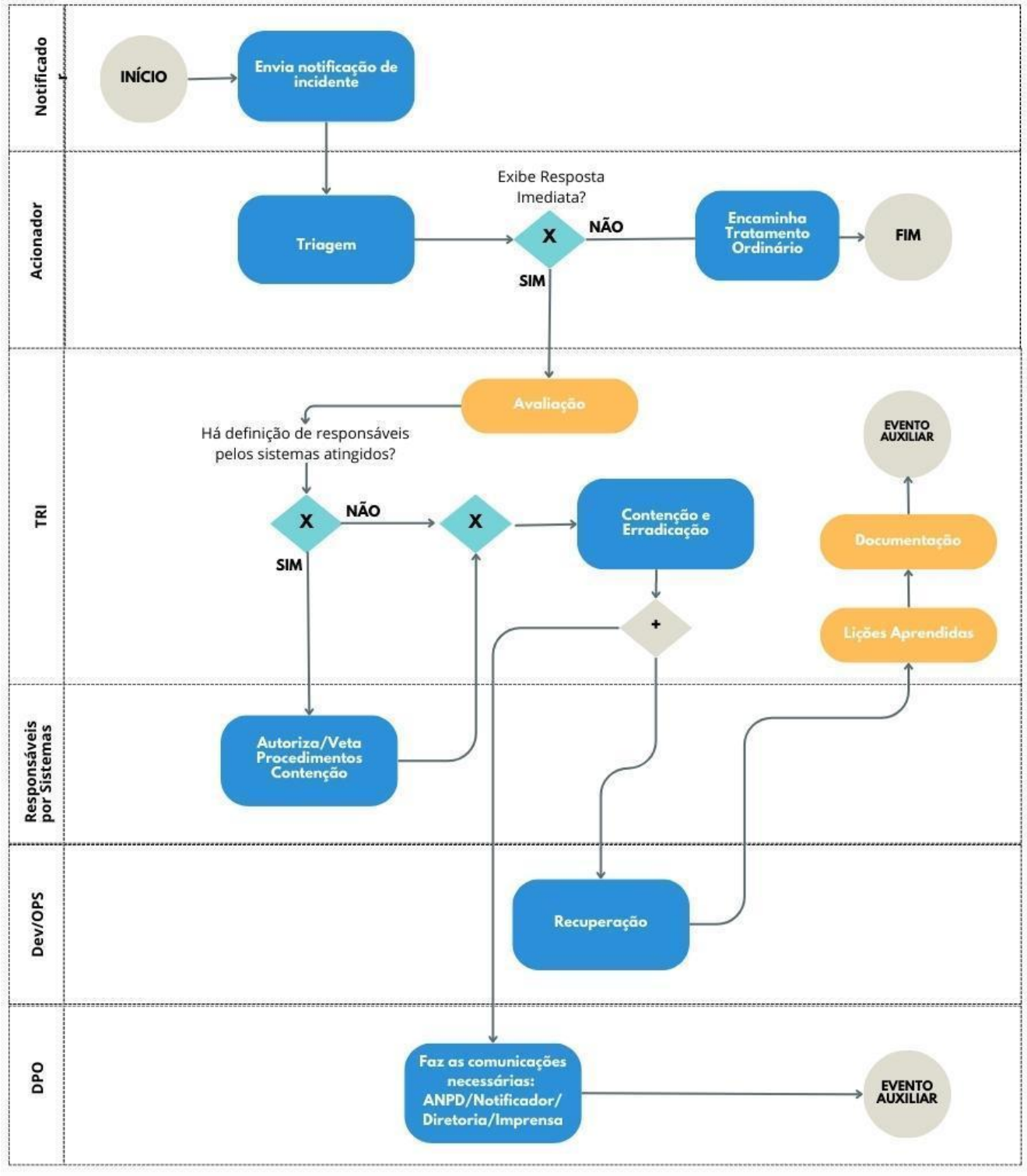
O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo. Descreve a forma como a Administração vai responder às situações de emergência e exceção. Pela potencial gravidade, a resposta deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência. Para o processo funcionar e ser estabelecido é pré-requisito a preparação prévia e contínua, atendendo os seguintes itens:

- Formação do Time de Resposta a Incidentes (TRI). Este é um grupo de empregados que deve ser designado através de Resolução de Diretoria, com acessos, habilidades, responsabilidades, treinamento e conhecimentos chave para responder aos mais variados tipos de incidentes. O TRI deve ter reuniões periódicas para definir melhorias neste plano, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo, bem como divulgação e treinamentos para os membros e demais empregados. O Encarregado pelo Tratamento de Dados Pessoais (DPO) e pelo menos um representante da Equipe de Segurança da Informação devem fazer parte desse grupo.
- Instalação e divulgação dos mecanismos de comunicação de incidente. Devem ser criadas, disponibilizadas e publicadas as formas de notificação à Companhia quando ocorrerem incidentes. O §1º, do Artigo 41, da Lei 13709/2018, a LGPD, estabelece: "A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador." Portanto, devem ser divulgados os e-mails: dpo@riodoscedros.com.br e ouvidoria@riodoscedros.sc.gov.br bem como os contatos do Callcenter. Deve haver indicação de quais mecanismos são considerados rápidos e seguros e se sugere o esclarecimento de quais as expectativas de anonimato que o notificador deve ter.
- Definição do grupo de Acionadores do TRI. Responsáveis por receberem as notificações e a realização do tratamento inicial. Para a cobertura 24 horas, este grupo deve incluir membros do Callcenter e contatos qualificados para executar a triagem.
- Instalação, configuração e definição de ferramentas de monitoria e alarmes. Devem informar diretamente o TRI através de mecanismos de comunicação direta como o Rocket Chat, WhatsApp ou SMS.
- Preparo de um Plano de Comunicação de Incidentes. Para facilitar a comunicação da Companhia deve ser criada uma biblioteca com modelos de documentos (templates) para comunicação formal do Encarregado pelo Tratamento de Dados Pessoais com a ANPD, titulares de dados, notificadores e imprensa.

Atores

- Notificador - pessoa ou sistema de monitoração que notifica incidente.
- TRI - Time de Resposta a Incidentes, definido na preparação prévia.
- Acionadores do TRI - grupo que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a importante cobertura 24 horas.
- Responsável por Sistema ou Controlador de Sistema, indicado que deve ser contatado e pode autorizar ou vetar procedimentos de emergência. Deve estar documentado, inclusive forma de contato para emergências.
- Equipe de Segurança da Informação.
- Encarregado pelo Tratamento de Dados Pessoais (DPO) - membro especial do TRI, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.
- Desenvolvedores/Operadores/Fornecedores dos sistemas - atuam no desenvolvimento de solução e instalação da mesma.

Diagrama BPMN do processo de resposta a incidentes.



Inicio

1) Um novo incidente é notificado, por pessoa externa ou não a Adminsitração Municipal ou por alarme da monitoração, usando um dos mecanismos de comunicação definidos. Notificação é recebida por Acionador do TRI.

Triagem

2) O Acionador do TRI deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.
3) Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.
4) Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares da Companhia pela Equipe de Segurança da Informação e Encarregado pelo Tratamento de Dados Pessoais, caso o incidente envolva dados pessoais.
5) Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o TRI deve ser acionado e passamos às fases seguintes.

Avaliação

6) Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do TRI a qualquer momento que julgar adequado e viável.

Contenção e Erradicação

7) Caso estejam identificados na CMDB, devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado na documentação, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.

8) O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida será realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas, colocação de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.
9) Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot das mesmas para posterior análise.

Recuperação

10) Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser iniciados, conforme especificado.

11) A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.
12) O TRI tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.
13) Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.
14) Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

Lições Aprendidas

15) Com o incidente contido e sua resolução encaminhada, o TRI deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos - inclusive deste Plano de Resposta a Incidentes.
16) As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

Documentação

17) O TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Comunicações

18) Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve avaliar e fazer as comunicações obrigatórias por Lei, se houverem, bem como informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANDP.