3. PARECERES

Neste capítulo, encontram-se os pareceres técnicos, documentos fundamentais e elaborados pela equipe técnica profissional e capacitada. Esse documento serve como um instrumento técnico, apresentando análises e conclusões sobre o programa de adequação da empresa Tombini e Cia Ltda , demonstrando a maturidade do processo ou situação.

Parecer Técnico da Área de Governança de Dados

Governança de Dados

A área de preocupação, denominada de Governança de Dados, está orientada a identificar e a analisar 04 (quatro) aspectos específicos, a saber:

1. O momento, quando da emissão deste parecer, em que a empresa se encontra frente ao Programa de Adequação à LGPD;
2. Quanto a atribuição de responsabilidade e evidenciação (veiculação) do Encarregado de Dados e Comitê Gestor de Proteção de Dados
3. Quanto a vinculação e disponibilização para eventuais consultas, de documentos que comprovem a jornada de adequação à LGPD;
4. Quanto a existência de um programa de capacitação dos colaboradores com foco na Lei Geral de Proteção de Dados - LGPD.

Condição Identificada

1. Quanto ao Programa de Adequação à LGPD

Em conformidade com as atividades já realizadas, a Tombini e Cia Ltda, encontra-se na fase de implantação/investimentos.

2. Quanto ao Encarregado de Dados e ao Comitê Gestor de Proteção de Dados

A Tombini e Cia Ltda, já atribuiu a responsabilidade de Encarregado de Dados mas ainda não houve a divulgação ao

público externo. A empresa também já constituiu a Comissão de Proteção de Dados Pessoais mas ainda não há um registro formal da nomeação do Cômite e das reuniões periódicas.

O encarregado de dados tem papel importantíssimo no escopo da proteção de dados da organização, além de atuar como um canal de comunicação entre o controlador de dados, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD), é ele a figura de maior responsabilidade na orientação dos funcionários e os operadores de dados quanto as boas práticas relativas à proteção de dados.

Já o Comitê Gestor de Proteção de Dados possuí a responsabilidade de avaliar os mecanismos de tratamento e proteção de dados existentes e propor ações de aperfeiçoamento.

3. Quanto aos documentos comprobatórios

No escopo da PRIVIA foram definidos como documentos comprobatórios essenciais: (1) política de privacidade; (2) plano de resposta à incidentes; (3) politica de segurança da informação.

A Política de Privacidade e Proteção de Dados encontra-se disponilizada no website institucional. No que tange Plano de resposta a incidentes e o canal de comunicação, informamos que as normas e diretrizes encontram-se disponiveis no âmbito interno da organização. Quanto à politica de segurança da informação, a mesma está em fase de desenvolvimento.

4. Quanto ao programa de capacitação dos colaboradores

Atualmente, o programa de capacitação dos colaboradores está em fase de desenvolvimento.

Preparar os colaboradores para que saibam como funciona o tratamento de dados pessoais conforme a legislação vigente é fundamental, além disso, o treinamento previne o mau uso de informações e minimiza chance de erros e incidentes de segurança.

Por fim, ainda com a capacitação, os colaboradores saberão como respeitar adequadamente os direitos dos titulares e o direito à proteção de dados pessoais.

Diante disso, é fundamental que a organização invista em um programa de capacitação eficiente, contemplando todos os seus colaboradores, evitando futuras sanções administrativas e judiciais, investimento este que vem ocorrendo na Tombini e Cia Ltda.

Esté o parecer.

Autor: Carolina Maciel em 27/09/2024 08:00

Parecer Técnico da Área de Processos e Procedimentos - ROPA

A área de preocupação, denominada de Áreas e Processos, está orientada a identificar e a analisar 11 (onze) aspectos específicos, a saber:

1. A posição do agente de tratamento de dados pessoais com relação ao processo analisado;
2. A identificação e qualificação de titulares e tipos de dados tratados;
3. A finalidade e base legal associada ao tratamento de dados pessoais;
4. A necessidade e gestão do consentimento no âmbito do processo analisado;
5. As condições e características afins a coleta de dados pessoais;
6. As condições e características do armazenamento de dados pessoais;
7. As condições de compartilhamento e transferências de dados

pessoais;
8. As exigências e condições de retenção dos dados pessoais;
9. As condições e características do descarte de dados pessoais;
10. Das possibilidades de correção e portabilidade dos dados pessoais; e
11. Da necessidade de LIA e Anonimização.

Condição Identificada

1. Posição do agente de tratamento de dados

A Tombini e Cia executa quase em sua totalidade, suas atividades na posição de Controlador de Dados Pessoais.

2. Quanto ao titulares e tipos de dados tratados

A organização trata dados de (1) público interno; (2) clientes; (3) fornecedores; (4) prestadores de serviços; (5) parceiros comerciais e (06) Público Externo. Sendo em grande maioria, dados pessoais classificados como comuns, tendo em vista a natureza da atividade desenvolvida pela organização.

3. Quanto a finalidade e base legal

Foi identificado que 67,82% dos processos analisados possuem explicitação da finalidade para o devido tratamento de dados pessoais, tendo em vista a nova Politica de Privacidade e Proteção de Dados, atualmente em processo de aprovação, bem como o fornecimento de cláusulas contratuais para inserção nos documentos.

Ademais, a totalidade dos processos mapeados, evidenciam como base legal para seus tratamentos de dados o cumprimento de obrigação legal e regulatória, execução de contratos e exercicio regular dos direitos. No mesmo sentido, a maioria dos dados coletados estão limitados ao mínimo necessário.

4. Quanto ao consentimento

Da totalidade dos processos mapeados, alguns possuem a necessidade de coleta de consentimento do titular de dados pessoais para o devido tratamento, sendo a coleta do presente consentimento realiza por formulários especificos.

5. Quanto a coleta de dados

A Tombini e Cia não faz uso de compra de dados, sendo a grande maioria das coletas executada através do fornecimento pelo próprio titular de dados.

6. Quanto ao armazenamento de dados

Os processos mapeados são armazenados em repositórios físicos e lógicos, de forma simultanea ou não.

O armazenamento digital ocorre mediante a utilização de sistemas informatizados (T4S, Questor, Avior, Ponto Secullum e etc).

O processo de segurança patrimonial, e backup encontra-se em estruturação baixa, motivo pelo qual. sugere-se o aprimoramento para que todas as medidas de mitigação de riscos sejam perfeitamente documentadas.

7. Quanto ao compartilhamento e transferência de dados

A Tombini e Cia realiza o compartilhamento das informações no âmbito interno da organização, para o perfeito cumprimento das atividades, isso ocorre entre as áreas operacionais e Comerciais, bem como com as áreas administrativas.

Tal compartilhamento ocorre por meio físico e lógico, através dos sistemas informatizados.

Além disso, a documentação física também está presente em maioria dentro do departamento pessoal e na execução dos trabalhos de alguns departamentos como: áreas de logística.

Já no que tange o compartilhamento externo, o mesmo ocorre

em nível nacional e internacional, seja através do uso de sistemas informatizados, parceiros comercial e instituições financeiras.

Por fim, ressalta-se que devido à natureza das atividades desenvolvidas pela Tombini e Cia, a organização está sujeita ao cumprimento de normas nacionais e internacionais, demandando compartilhamento de informações, sobretudo à órgãos governamentais e empresas certificadoras.

8. Sobre a retenção de dados pessoais

Sobre a retenção de dados pessoais, considera-se que aqueles pertinentes ao desenvolvimento das atividades da organização, em especial as que tem abrangência técnica relacionada a atividade desenvolvida necessitam de maior tempo de armazenamento em virtude de cumprimento de obrigação legal regulatória.

Outrossim, dados fiscais, contábeis, trabalhistas e previdenciarios, também demandam maior atenção quando ao tempo de guarda.

Constatou-se através das entrevistas realizadas, que atualmente 91,95% dos dados pessoais tratados permanecem sob a guarda da Tombini e Cia por tempo indeterminado.

Entretanto, ressalta-se que a organização não possuí política ou normativa interna contendo tabela de temporalidade dos processos e procedimentos de retenção, a determinação do tempo de guarda é relativa ao espaço e organização interna de cada departamento.

9. Descarte de dados

Este é o principal ponto de atenção decorrente da análise dos dados mapeados, tendo em vista a Tombini e Cia não possui procedimento de descarte de dados de forma documentada, o mesmo ocorre através da organização interna de cada departamento, sendo que somente 6,9% possuí resposta positiva quanto ao descarte.

A documentação física é descartada em virtude de necessidade de abertura de espaço nos departamentos e no arquivo geral da organização, e ocorre através do descarte em lixo comum ou quando muito, por picotadeira de papel.

Diante disso, junto a Politica de retenção, armazenamento, anonimização e descarte, é necessária a elaboração de plano de descarte de dados pessoais de forma eficiente a evidenciar esse procedimento.

10. Quanto a correção e portabilidade de dados

No que se refere a possibilidade de acesso e correção, a Tombini e Cia possui a possibilidade de correção parcial dos dados, somente nos casos de divergência de informações, erros de digitação, bem como atualizações cadastrais, não sendo possível por outro lado, a correção dos dados coletados e gerados por órgãos oficiais.

Quanto à portabilidade dos dados, a mesma somente ocorre em processos e procedimentos quase em sua totalidade.

Por fim, no caso de procedimentos que não possibilitam a portabilidade, foram sugeridas análises complementares para possibilitar a portabilidade de dados, em atendimento à exigência da LGPD.

11. Quanto à análise de Legitimo Interesse (LIA) e Anonimização de dados pessoais

Os procedimentos de tratamentos de dados pessoais relativos as atividades desenvolvidas pela Tombini e Cia somente 01 abrange a aplicação do Legitimo Interesse, sendo realizada, portanto, a análise complementar.

Já sobre o procedimento de anonimização,não foram identificados processos pertinentes ao procedimento.

Este é o parecer.

Autor: Carolina Maciel em 27/09/2024 08:52

Parecer Técnico sobre Tempo de Retenção

Tempo de Retenção/Armazenamento e Compartilhamento/ Transferência de dados em virtude de Obrigação Legal e Regulatória

---

O Art. 7° da LGPD, II dispõe: “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] II – para o cumprimento de obrigação legal ou regulatória pelo controlador [...]”.

Para que seja possível que o controlador legitime o tratamento de dados pessoais que realiza por meio desta base legal, é preciso justificar a utilização do dado pessoal para atender uma obrigação legal ou regulatória.

Condição Identificada

A Privia identificou que 28,74% dos processos mapeados necessitam manter o armazenamento dos dados em virtude de obrigação legal e regulatória, bem como, obrigam a transferência externa dos dados à órgãos públicos, instituições financeiras e sindicatos (quando for o caso).

A legislação determina a guarda documentos para fins, fiscais, tributários, trabalhistas e previdenciários.

O período de guarda dos documentos relacionados com os tributos no prazo de decadência e prescrição, previstos nos

artigos 173 e 174 do Código Tributário Nacional (CTN), é de 05 anos, senão vejamos:

Art. 173. O direito de a Fazenda Pública constituir o crédito tributário extingue-se após 5 (cinco) anos, contados:
I – em primeiro lugar, aos débitos por obrigação própria, e em segundo lugar aos decorrentes de responsabilidade tributária;
II – primeiramente, às contribuições de melhoria, depois às taxas e por fim aos impostos;
III – na ordem crescente dos prazos de prescrição;
IV – na ordem decrescente dos montantes.

Art.174. A ação para a cobrança do crédito tributário prescreve em cinco anos, contados da data da sua constituição definitiva. III – de exigência, por mais de uma pessoa jurídica de direito público, de tributo idêntico sobre um mesmo fato gerador.
Prescrição é o decurso do prazo de cinco anos para cobrar judicialmente o tributo devido. No fim desse prazo, o crédito tributário será extinto (art. 156, v, do CTN) e não mais poderá ser exigido pelo Fisco.

O mesmo prazo se aplica aos livros obrigatórios e comprovantes de lançamento.

Já o artigo 195 do Código Tributário Nacional (CTN), prevê:

Art.195. Para os efeitos da legislação tributária, não têm aplicação quaisquer disposições legais excludentes ou limitativas do direito de examinar mercadorias, livros, arquivos, documentos, papéis e efeitos comerciais ou fiscais, dos comerciantes industriais ou produtores, ou da obrigação destes de exibi-los.

Já os documentos trabalhistas e previdenciários possuem prazo de guarda que varia de 2 a 30 anos, não havendo uma regra específica, ficando a cargo do empregador adotar um critério mais conservador possível, entretanto a Constituição Federal elenca a seguinte disposição:

"Art. 7° São direitos dos trabalhadores urbanos e rurais, além de

outros que visem à melhoria de sua condição social: [...]XXIX – ação, quanto aos créditos resultantes das relações de trabalho, com prazo prescricional de cinco anos para os trabalhadores urbanos e rurais, até o limite de dois anos após a extinção do contrato de trabalho;(Redação Emenda Constitucional nº 28 de 25/5/00). [...]"

Quanto aos documentos previdenciários, o Decreto 3.048/99, prevê a obrigatoriedade de a empresa manter à disposição da fiscalização, durante dez anos, os documentos comprobatórios do cumprimento de suas obrigações legais, inclusive os arquivos digitais do sistema de processamento eletrônico de dados trabalhistas e previdenciários.

A Lei Geral de Proteção de Dados possui legislação específica sobre políticas de armazenamento de dados que variam de acordo com as necessidades de cada ramo de atividade empresarial. Logo, podem haver limites mais rígidos para a extensão de dados, bem como o período que eles podem ser armazenados antes de serem apagados. Por isso é fundamental avaliar se os dados trazem interferência nos resultados econômicos fiscais a empresa em se tratando de arquivos de documentos tributários, fiscais, trabalhistas e previdenciários.

Oportuno ainda mencionar que: caso a empresa tenha algum processo fiscal em andamento, seja pessoa fiscalizada ou como autor do processo, esta não poderá descartar os documentos até que o processo esteja concluindo, tanto na esfera administrativa como na esfera judicial. O período para contagem da prescrição é iniciada a partir do encerramento do ano fiscal, como por exemplo: este ano (2022) prescreve-se para impostos federais o ano de 2017.

Abaixo, relação de documentos e prazos de guarda, exigidos pela legislação:

Comerciais e Fiscais
Prazo 20 anos

- Compensação Mercantil;
- Contrato de Seguro/ Informação de Valores;
- Contrato de Seguro Pessoal;
- Contratos previdenciários privados;
- Novação e Pagamentos Mercantis;
- Títulos de Capitalização.

Prazo 08 anos

- Títulos ou Contratos de Investimentos Coletivos;

Prazo Indeterminado

- Ações Judiciais e/ou Administrativas

Tributário
Prazo 05 anos

- Notas fiscais e recibos;
- Livros Fiscais;
- IR - Imposto de Renda;
- CSLL - Contribuição Social Sobre o Lucro Líquido;
- PIS - Programa de Integração Social;
- COFINS - Contribuição para Financiamento da Seguridade Social;
- ICMS - Imposto sobre Circulação de Mercadorias e Sobre Prestação de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação;
- Declarações: DIPJ, DCTF, DACON;
- DASN - Declaração Anual do Simples Nacional;
- DIRF - Declaração do Imposto Retido na Fonte;
- Declaração de Ajuste Anual - IRPF e Deduções;
- GIA - Guia de Informação e Apuração do ICMS.

Trabalhista e Previdenciário
Prazo 30 anos

- FGTS - Fundo de Garantia do Tempo de Serviços;
- GFIP - Guia de Recolhimento do FGTS e Informações à Previdência Social;

- GRFC - Guia de Recolhimento Rescisório do FGTS e da Contribuição Social;
- Comprovantes de Depósito do FGTS

Prazo 20 anos

- PPP - Perfil Profissiográfico Previdenciário;
- PCMSO - Programa de Controle Médico de Saúde Ocupacional;

Prazo 10 anos

- Folha de Pagamento;
- Sistema Eletrônico de Dados Trabalhistas e Previdenciários;
- CAT - Comunicação de Acidentes de Trabalho;
- GPS - Guia de Previdência Social.
- Guia de Previdência Social.

Prazo 05 anos

- GRCSU - Contribuição Sindical;
- Recibo de Pagamento de Salário, Férias, 13° e Controle de Ponto;
- CAGED - Cadastro Geral de Empregados e Desempregados;
- Relação Anual de Informações Sociais (RAIS).

Prazo 02 anos

- Termo de Rescisão do Contrato de Trabalho, Pedido de Demissão e Aviso Prévio.

Prazo Indeterminado

- Contrato de Trabalho;
- Livro ou Ficha de Registro de Empregado

Atualmente, é permitido que as empresas armazenem a documentação eletronicamente, seja em mídias fiscais - Pendrives e HDs Externos, Servidores Externos e Internos -, e em plataformas de armazenamento na nuvem.

Essa documentação deve ser armazenada em meio eletrônico, ótico ou equivalente, tendo o mesmo valor probatório do original para fins de prova em procedimentos de fiscalização. Contudo, é importante que o cliente/empresário assegure a guarda dos arquivos digitais durante um período, mantendo uma cópia de segurança e consultando o entendimento dos fiscos estadual e municipal antes de destruir os documentos físicos.

No caso do compartilhamento interno, é necessário que ocorra para o cumprimento da prestação de serviços de garantia, compras entre outros, tendo em vista que essa prestação de serviços abrange inúmeros departamentos da Tombini e Cia.

Por fim, no que tange o compartilhamento externo, o mesmo é efetuado por força de obrigação legal e regulatória junto à diversos órgãos públicos, instituições bancárias e sindicatos (quando for o caso), cuja as legislações pertinentes já se encontram listadas anteriormente.

Diante disso, serão recomendadas ações para devida comprovação de todas as obrigações regulatórias e setoriais, a serem anexadas ao RIPD.

Autor: Carolina Maciel em 27/09/2024 08:58

Parecer Técnico de Análise dos Operadores de Dados

A área de preocupação, denominada de Análise de Operadores de Dados / Parceiros , está orientada a identificar e a analisar como, no âmbito de suas responsabilidades, dados pessoais eventualmente compartilhados pela a empresa são tratados.

Condição Identificada

Para fins desta análise os fornecedores e/ou parceiros que, diretamente, se relacionam com a Tombini e Cia foram organizados separadamente, cada um com seu formulário individual.

A Tombini e Cia, também utiliza serviços de oficinas terceirizadas, bem como fornecedores de transporte, rastreios, controles de ponto e etc.

Registra-se que todas as informações existentes (conforme exige a lei) foram obtidas nos portais de cada um dos fornecedores, mediante divulgação voluntária. O que de antemão já fornece um panorama de como o fornecedor tem efetuado ou não o cumprimento da legislação.
No caso dos fornecedores cujas informações eram mínimas ou inexistentes, foram efetuados contatos via telefone, na intenção de solicitar as informações por e-mail ou através de realização de videoconferência, contudo, os contatos se mostraram inexitosos.

Para os fornecedores classificados como de risco critico ou grave, serão recomendadas ações de aprimoramento e adequação à LGPD.

Autor: Carolina Maciel em 27/09/2024 09:09

Parecer Técnico sobre Programa de Capacitação de Colaboradores quanto ao Programa de Proteção de Dados da Organização

Capacitação dos Colaboradores

A conformidade com a Lei Geral de Proteção de Dados exige mais do que o ato de executar o mapeamento de dados, revisão de contratos e implementação de sistemas de segurança da informação.

Para um efetivo cumprimento da legislação é necessário que todos os colaboradores estejam cientes da importância da proteção de dados e do seu próprio papel no processo.

Em 2021, uma pesquisa liderada pela Deloitte promovida em 122 empresas apontou que em 76% dessas organizações, o investimento em treinamentos e politicas de segurança cibernética proporcionaram maior transparência nas decisões estratégicas nas organizações.

Entre as principais práticas de segurança cibernética, o investimento na capacitação dos colaboradores ficou em 2° lugar, com 44%, ficando somente atrás de Governança e Administração de Acessos com 61%.
Investir na capacitação dos colaborares da Tombini e Cia pode trazer inúmeras vantagens para a organização, contudo, para melhor elucidar os benefícios dessa prática, destacam-se 05 vantagens indiscutíveis:

1. Melhor relacionamento com o cliente;
2. Aumento da segurança jurídica;
3. Demonstrar a conformidade com a Lei, aumenta a reputação da empresa;
4. Otimiza a ética profissional;
5. Estar em conformidade é competitivo.

Condição Identificada

A Privia identificou que:

No decorrer das entrevistas promovidas junto aos colaboradores da Tombini e Cia, percebeu-se que os colaboradores de modo geral não possuíam nenhuma familiaridade com a Lei Geral de Proteção de Dados - LGPD, o que em alguns aspectos dificultou em um primeiro momento a identificação de procedimentos internos específicos dentro da organização.

Contudo, mesmo sem terem um conhecimento básico da legislação, todos se mostraram bastante interessados em entenderem a demanda e responderem as questões da maneira mais clara e abrangente que foi possível, o que podemos relacionar de antemão como um ponto positivo entre os colaboradores envolvidos.

É sempre de suma importância que haja comprometimento dos colaboradores para o devido cumprimento da legislação da melhor forma possível, sendo que tal comprometimento somente é passível de ser conseguido através de uma proposta de capacitação condizente com a realidade da organização.

Para isso, é preciso que a organização invista em programas de capacitação adequados ao perfil da organização de modo geral, respeitando obviamente as peculiaridades de cada colaborador e as funções exercidas, bem como escopo obrigacional de cada procedimento de tratamento de dados pessoais.

Vale ressaltar que o primeiro passo para a correta implementação da Lei Geral de Proteção de Dados é a conscientização, passando por todos os colaboradores e refletindo nos prestadores de serviço e fornecedores. Desta forma, a LGPD deixará de ser um fim e passará a ser um sistema continuo de busca por soluções que tragam maior segurança não só aos clientes mas também a todos os envolvidos direta e indiretamente com a organização.

É preciso ter em mente que grande parte dos incidentes de segurança não são ocasionados por hackers, mas sim por colaboradores, em grande maioria, de forma involuntária.

Além disso, a conscientização faz parte de um dos controles de

segurança da informação presentes na ISO 27001, e é somente através de um treinamento adequada é que a organização terá uma base solida para responder de forma efetiva aos incidentes de segurança, tendo em vista que não é somente o profissional do TI e o DPO que são responsáveis pela proteção de dados, mas sim, uma responsabilidade de todos.

Como foco de disseminação da cultura de proteção de dados, a organização deve adotar um olhar amplo e entender no mínimo os três grandes pilares que fazem parte de um efetivo sistema de segurança da informação: Pessoas; Processos e Tecnologias.

Ademais, é preciso que a organização esteja atenta à 03 pontos importantes quando falamos de implementação à Lei Geral de Proteção de Dados.

1. Embora o Relatório de Impacto e Proteção de Dados - RIPD, seja um documento essencial para demonstrar o comprometimento da empresa quanto à execução de implementação da LGPD, somente ele, por si só não comprova que a empresa está 100% adequada à lei. Provar estar em *Compliance* -, com a legislação é algo à ser incorporado através de uma gestão de processos e evidencias;
2. A implementação é artesanal e única para cada empresa, observando as peculiaridades do negócio;
3. Após identificar as peculiaridades, busque propostas e situações de conscientização que estejam alinhados com o contexto da empresa.

Outra metodologia a ser aplicada nos programas de conscientização é a Governança Corporativa que é capaz de assegurar não só a conscientização adequada dos colaboradores, prestadores de serviços e fornecedores, mas também os interesses dos administradores/sócios, garantindo que os processos e as estratégias pré-estabelecidas estão sendo corretamente seguidas, promovendo concomitantemente uma cultura de prestação de contas dentro da empresa.

A própria Lei Geral de Proteção de Dados possibilita que os controladores e operadores de dados criem práticas de Governança Corporativa afim de estabelecerem: Códigos de Conduta; Organização; Procedimentos Internos; Normas de Segurança; Padrões Técnicos; Obrigações; Ações Educativas; Mecanismos de Supervisão; Mitigação de Riscos.

Diante disso, é importante estruturar um processo de capacitação com a seguinte cronologia:

1. Planejamento

Defina a estrutura da capacitação, e como ela será realizada: departamentos ou módulos (lembre-se a capacitação nunca deve ser realizada uma única vez); e estabeleça os assuntos mais relevantes em conformidade com o modelo de negócios da Renault Criciúma - Matriz.
Determine metas e teste seus colaboradores periodicamente.

2. Teoria e Prática

Utilize conteúdos e técnicas que mesclem teoria e prática. Cite a legislação, mas utilize exemplos práticos.

3. Uso de Tecnologias

Use a tecnologia a favor da sua organização, faça uso de plataformas de capacitação, treinamento e gamificação, capazes de englobar, vídeos, testes, jogos etc. Além de facilitar o processo, cria uma cultura de tecnologia na empresa.

Em recomendações técnicas apresentaremos opções de serviços e sistemas para melhor aproveitamento.

Autor: Carolina Maciel em 27/09/2024 09:11

A área de preocupação, denominada de Segurança de Informações, está orientada a identificar e a analisar 04 (quatro) controles especificos:

1. Operacionais;
2. Pessoas;
3. Físicos;
4. Tecnológicos.

Condição Identificada

1. No escopo dos controles operacionais, responsável pela análise dos critérios:

(a) Políticas de Segurança da Informação;
(b) Papeis e Responsábilidades;
(c) Segregação de Funções;
(d) Responsabilidade da Diretoria;
(e) Inteligência de Ameaças;
(f) Inventário de Informações;
(g) Uso Aceitável de Informações;
(h) Devolução de Ativos;
(j) Classificação de Informações;
(k) Transferência de Informações;
(l) Controle de Acessos;
(m) Gestão de Identidades;
(n) Informações de Autenticação;
(o) Direitos de Acesso;
(p) Segurança de Informação nas Relações com Fornecedores;
(q) Segurança da Informação para o Uso de Serviços em Nuvem;
(r) Planejamento e Preparação da Gestão de Incidentes de Segurança da Informação;
(s) Avaliação e Decisão Sobre Eventos de Segurança da Informação;
(t) Prontidão de TIC para Continuidade de Negócios;

(u) Requisitos Legais, Estatutários, Regulamentáres e Contratuais.

Os controles operacionais da segurança da informação são medidas implementadas para proteger dados e infraestrutura de TI contra ameaças e riscos. Eles podem ser classificados em várias categorias, incluindo:

1. **Controles Preventivos**: Projetados para evitar que incidentes de segurança ocorram. Exemplos incluem políticas de segurança, treinamento de funcionários e autenticação multifator.
2. **Controles Detectivos**: Ajudam a identificar e detectar incidentes de segurança quando eles ocorrem. Exemplos incluem sistemas de detecção de intrusão e monitoramento de logs.
3. **Controles Corretivos**: Implementados para corrigir falhas de segurança e restaurar sistemas após um incidente. Exemplos incluem planos de resposta a incidentes e backups de dados.
4. **Controles Físicos**: Protegem o acesso físico aos recursos de TI, como fechaduras, câmeras de vigilância e guardas de segurança.
5. **Controles Técnicos**: Envolvem o uso de tecnologia para proteger sistemas e dados, como firewalls, antivírus e criptografia.

Dos controles listados acima:

00 foram classificados como risco leve
04 foram classificados como risco moderado
05 foram classificados como fisco grave
13 foram classificados como risco crítico

2. No escopo do controle de pessoas, é realizada a análise dos seguintes critérios:

(a) Seleção
(b) Termos e Condições de Contratação;
(c) Conscientização, Educação e Treinamento em Segurança da

Informação;
(d)Processo Disciplinar;
(e) Acordos de Confidencialidade ou não Divulgação;
(f) Trabalho Remoto;
(g) Relato de Eventos de Segurança da Informação;

Os controles de pessoas na segurança da informação são medidas focadas em gerenciar e monitorar o comportamento humano para proteger dados e sistemas. Aqui estão alguns exemplos importantes:

1. **Treinamento e Conscientização**: Programas regulares para educar os funcionários sobre práticas seguras, políticas de segurança e como reconhecer ameaças como phishing.
2. **Políticas de Segurança**: Regras e diretrizes claras que definem o que é permitido e o que não é, ajudando a alinhar o comportamento dos funcionários com os objetivos de segurança da organização.
3. **Controle de Acesso**: Garantir que os funcionários tenham acesso apenas às informações e sistemas necessários para suas funções, minimizando o risco de acesso não autorizado.
4. **Segregação de Funções**: Dividir responsabilidades entre diferentes pessoas para reduzir o risco de fraude ou erro, garantindo que nenhuma pessoa tenha controle total sobre um processo crítico.
5. **Monitoramento e Auditoria**: Revisar regularmente as atividades dos funcionários para detectar comportamentos suspeitos ou não conformes.

Esses controles são essenciais para criar uma cultura de segurança dentro da organização e proteger contra ameaças internas e externas.

Dos controles listados acima:

03 foram classificados como risco leve
01 foram classificados como risco moderado
02 foram classificados como fisco grave
02 foram classificados como risco crítico

3. No âmbito dos Controles Físicos, foram análisados os critérios:

(a) Perimetros de Segurança Física;
(b) Entrada Física;
(c) Segurança de Escritórios, Salas e Instalações;
(d) Monitoramento de Segurança Física;
(e) Segurança de Ativos fora das Instalações da Organização;

Os controles físicos da segurança da informação são medidas tangíveis implementadas para proteger os ativos e as pessoas dentro de uma organização. Aqui estão alguns exemplos comuns:

1. **Câmeras de Segurança**: Monitoram e registram atividades em áreas sensíveis para prevenir e detectar acessos não autorizados.
2. **Portas e Fechaduras**: Restringem o acesso físico a áreas críticas, garantindo que apenas pessoas autorizadas possam entrar.
3. **Guardas de Segurança**: Pessoal treinado para monitorar e proteger instalações contra ameaças físicas.
4. **Alarmes de Incêndio e Fumaça**: Detectam e alertam sobre incêndios, permitindo uma resposta rápida para proteger pessoas e ativos.
5. **Sistemas de Controle de Acesso**: Utilizam cartões de acesso, biometria ou códigos para controlar quem pode entrar em determinadas áreas.
6. **Cercas e Muros**: Criam barreiras físicas para impedir o acesso não autorizado a instalações.

Esses controles são essenciais para garantir a segurança física dos recursos de TI e das informações sensíveis da organização

Dos controles listados acima:

01 foram classificados como risco leve
00 foram classificados como risco moderado
03 foram classificados como fisco grave
01 foram classificados como risco crítico

4. Por fim, no âmbito dos Controles Tecnológicos, foram

análisados os critérios:

(a) Dispositivos de Endpoint do Usuário;
(b) Direitos de Acessos Privilegiados;
(c) Restrição de Acesso à Informação;
(d)Autenticação Segura;
(e) Prevenção contra Malwere;
(f) Gestão de Vulnerabilidades Técnicas;
(g) Exclusão de Informações;
(h) Mascaramento de Dados;
(i) Prevenção de Vazamentos de Dados;
(j) Backup de Informações;
(k) Redundância de Recursos para Tratamento de Informações;
(l) Log;
(m) Atividades de Monitoramento.

Os controles tecnológicos de segurança da informação são medidas implementadas para proteger sistemas, redes e dados contra ameaças cibernéticas. Aqui estão alguns exemplos importantes:

1. **Firewalls**: Dispositivos ou softwares que monitoram e controlam o tráfego de rede com base em regras de segurança predefinidas.
2. **Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS)**: Monitoram a rede ou sistemas para atividades maliciosas ou violações de políticas e podem tomar ações para prevenir essas ameaças.
3. **Antivírus e Antimalware**: Programas que detectam, previnem e removem softwares maliciosos de computadores e redes.
4. **Criptografia**: Técnica que codifica dados para que apenas pessoas autorizadas possam acessá-los, garantindo a confidencialidade e integridade das informações.
5. **Autenticação Multifator (MFA)**: Requer que os usuários forneçam duas ou mais formas de verificação antes de acessar sistemas ou dados, aumentando a segurança.
6. **Gerenciamento de Identidade e Acesso (IAM)**: Ferramentas e políticas que garantem que as pessoas certas tenham o

acesso apropriado aos recursos certos no momento certo.

7. **Soluções de Detecção e Resposta de Endpoint (EDR)**: Monitoram continuamente os endpoints para detectar e responder a atividades suspeitas.

Esses controles são essenciais para proteger a infraestrutura de TI e os dados sensíveis contra uma variedade de ameaças cibernéticas.

Dos controles listados acima:

02 foram classificados como risco leve
01 foram classificados como risco moderado
04 foram classificados como fisco grave
06 foram classificados como risco crítico

Este é o parecer.

Autor: Carolina Maciel em 27/09/2024 09:12

Parecer Técnico da Área de Governança de Dados - 2026

Governança de Dados

A área de preocupação, denominada de Governança de Dados, está orientada a identificar e a analisar 04 (quatro) aspectos específicos, a saber:

1. O momento, quando da emissão deste parecer, em que a empresa se encontra frente ao Programa de Adequação à LGPD;
2. Quanto a atribuição de responsabilidade e evidenciação (veiculação) do Encarregado de Dados e Comitê Gestor de Proteção de Dados
3. Quanto a vinculação e disponibilização para eventuais consultas, de documentos que comprovem a jornada de adequação à LGPD;
4. Quanto a existência de um programa de capacitação dos colaboradores com foco na Lei Geral de Proteção de Dados - LGPD.

Condição Identificada

1. Quanto ao Programa de Adequação à LGPD

Em conformidade com as atividades já realizadas, a Tombini e Cia Ltda, encontra-se na fase de implantação/investimentos.

2. Quanto ao Encarregado de Dados e ao Comitê Gestor de Proteção de Dados

A Tombini e Cia Ltda. já atribuiu formalmente a responsabilidade pelo Encarregado de Dados, cujas informações encontram-se divulgadas ao público externo por meio da Política de Privacidade disponibilizada no website institucional. A empresa também já constituiu formalmente o Comitê Gestor de Proteção de Dados, com a definição dos respectivos responsáveis.

O encarregado de dados tem papel importantíssimo no escopo da proteção de dados da organização, além de atuar como um canal de comunicação entre o controlador de dados, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD), é ele a figura de maior responsabilidade na orientação dos funcionários e os operadores de dados quanto as boas práticas relativas à proteção de dados.

Já o Comitê Gestor de Proteção de Dados possuí a

responsabilidade de avaliar os mecanismos de tratamento e proteção de dados existentes e propor ações de aperfeiçoamento.

3. Quanto aos documentos comprobatórios

No escopo da PRIVIA foram definidos como documentos comprobatórios essenciais: (1) política de privacidade; (2) plano de resposta à incidentes; (3) politica de segurança da informação.

A Política de Privacidade e Proteção de Dados encontra-se disponibilizada no website institucional. O Plano de Resposta a Incidentes e o canal de comunicação também estão formalizados e disponíveis no âmbito interno da organização. A Política de Segurança da Informação, bem como as demais políticas e normas relacionadas à proteção de dados pessoais, encontram-se formalizadas e disponíveis internamente, compondo o conjunto de documentos que orientam as práticas de proteção de dados da organização.

4. Quanto ao programa de capacitação dos colaboradores

A Tombini e Cia Ltda. já realizou treinamentos de capacitação e conscientização dos colaboradores quanto à proteção de dados pessoais e às disposições da legislação vigente.

A capacitação dos colaboradores é fundamental para orientar quanto ao correto tratamento de dados pessoais, contribuindo para a prevenção do uso inadequado de informações, a redução de erros e a minimização de riscos relacionados a incidentes de segurança.

Além disso, os treinamentos contribuem para que os colaboradores compreendam suas responsabilidades no tratamento de dados pessoais e observem adequadamente os direitos dos titulares e os princípios relacionados à proteção de dados pessoais.

Diante disso, destaca-se a importância da continuidade das ações de capacitação e conscientização, de forma periódica e compatível com as atividades desempenhadas pelos

colaboradores, visando ao fortalecimento contínuo da cultura de proteção de dados na organização.

Esté o parecer.

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 12:00

Parecer Técnico Controles de SI | TI - 2026

A área de preocupação, denominada de Segurança de Informações, está orientada a identificar e a analisar 04 (quatro) controles especificos:

1. Operacionais;
2. Pessoas;
3. Físicos;
4. Tecnológicos.

Condição Identificada

1. No escopo dos controles operacionais, responsável pela análise dos critérios:

(a) Políticas de Segurança da Informação;
(b) Papeis e Responsábilidades;
(c) Segregação de Funções;
(d) Responsabilidade da Diretoria;
(e) Inteligência de Ameaças;
(f) Inventário de Informações;
(g) Uso Aceitável de Informações;
(h) Devolução de Ativos;
(j) Classificação de Informações;

(k) Transferência de Informações;
(l) Controle de Acessos;
(m) Gestão de Identidades;
(n) Informações de Autenticação;
(o) Direitos de Acesso;
(p) Segurança de Informação nas Relações com Fornecedores;
(q) Segurança da Informação para o Uso de Serviços em Nuvem;
(r) Planejamento e Preparação da Gestão de Incidentes de Segurança da Informação;
(s) Avaliação e Decisão Sobre Eventos de Segurança da Informação;
(t) Prontidão de TIC para Continuidade de Negócios;
(u) Requisitos Legais, Estatutários, Regulamentáres e Contratuais.

Os controles operacionais da segurança da informação são medidas implementadas para proteger dados e infraestrutura de TI contra ameaças e riscos. Eles podem ser classificados em várias categorias, incluindo:

1. **Controles Preventivos**: Projetados para evitar que incidentes de segurança ocorram. Exemplos incluem políticas de segurança, treinamento de funcionários e autenticação multifator.
2. **Controles Detectivos**: Ajudam a identificar e detectar incidentes de segurança quando eles ocorrem. Exemplos incluem sistemas de detecção de intrusão e monitoramento de logs.
3. **Controles Corretivos**: Implementados para corrigir falhas de segurança e restaurar sistemas após um incidente. Exemplos incluem planos de resposta a incidentes e backups de dados.
4. **Controles Físicos**: Protegem o acesso físico aos recursos de TI, como fechaduras, câmeras de vigilância e guardas de segurança.
5. **Controles Técnicos**: Envolvem o uso de tecnologia para proteger sistemas e dados, como firewalls, antivírus e criptografia.

Dos controles listados acima:

21 foram classificados como risco leve
01 foram classificados como risco moderado
00 foram classificados como fisco grave
00 foram classificados como risco crítico

2. No escopo do controle de pessoas, é realizada a análise dos seguintes critérios:

(a) Seleção
(b) Termos e Condições de Contratação;
(c) Conscientização, Educação e Treinamento em Segurança da Informação;
(d)Processo Disciplinar;
(e) Acordos de Confidencialidade ou não Divulgação;
(f) Trabalho Remoto;
(g) Relato de Eventos de Segurança da Informação;

Os controles de pessoas na segurança da informação são medidas focadas em gerenciar e monitorar o comportamento humano para proteger dados e sistemas. Aqui estão alguns exemplos importantes:

1. **Treinamento e Conscientização**: Programas regulares para educar os funcionários sobre práticas seguras, políticas de segurança e como reconhecer ameaças como phishing.
2. **Políticas de Segurança**: Regras e diretrizes claras que definem o que é permitido e o que não é, ajudando a alinhar o comportamento dos funcionários com os objetivos de segurança da organização.
3. **Controle de Acesso**: Garantir que os funcionários tenham acesso apenas às informações e sistemas necessários para suas funções, minimizando o risco de acesso não autorizado.
4. **Segregação de Funções**: Dividir responsabilidades entre diferentes pessoas para reduzir o risco de fraude ou erro, garantindo que nenhuma pessoa tenha controle total sobre um processo crítico.
5. **Monitoramento e Auditoria**: Revisar regularmente as atividades dos funcionários para detectar comportamentos suspeitos ou não conformes.

Esses controles são essenciais para criar uma cultura de segurança dentro da organização e proteger contra ameaças internas e externas.

Dos controles listados acima:

07 foram classificados como risco leve
00 foram classificados como risco moderado
00 foram classificados como fisco grave
00 foram classificados como risco crítico

3. No âmbito dos Controles Físicos, foram análisados os critérios:

(a) Perimetros de Segurança Física;
(b) Entrada Física;
(c) Segurança de Escritórios, Salas e Instalações;
(d) Monitoramento de Segurança Física;
(e) Segurança de Ativos fora das Instalações da Organização;

Os controles físicos da segurança da informação são medidas tangíveis implementadas para proteger os ativos e as pessoas dentro de uma organização. Aqui estão alguns exemplos comuns:

1. **Câmeras de Segurança**: Monitoram e registram atividades em áreas sensíveis para prevenir e detectar acessos não autorizados.
2. **Portas e Fechaduras**: Restringem o acesso físico a áreas críticas, garantindo que apenas pessoas autorizadas possam entrar.
3. **Guardas de Segurança**: Pessoal treinado para monitorar e proteger instalações contra ameaças físicas.
4. **Alarmes de Incêndio e Fumaça**: Detectam e alertam sobre incêndios, permitindo uma resposta rápida para proteger pessoas e ativos.
5. **Sistemas de Controle de Acesso**: Utilizam cartões de acesso, biometria ou códigos para controlar quem pode entrar em determinadas áreas.
6. **Cercas e Muros**: Criam barreiras físicas para impedir o acesso

não autorizado a instalações.

Esses controles são essenciais para garantir a segurança física dos recursos de TI e das informações sensíveis da organização

Dos controles listados acima:

05 foram classificados como risco leve
00 foram classificados como risco moderado
00 foram classificados como fisco grave
00 foram classificados como risco crítico

4. Por fim, no âmbito dos Controles Tecnológicos, foram análisados os critérios:

(a) Dispositivos de Endpoint do Usuário;
(b) Direitos de Acessos Privilegiados;
(c) Restrição de Acesso à Informação;
(d)Autenticação Segura;
(e) Prevenção contra Malwere;
(f) Gestão de Vulnerabilidades Técnicas;
(g) Exclusão de Informações;
(h) Mascaramento de Dados;
(i) Prevenção de Vazamentos de Dados;
(j) Backup de Informações;
(k) Redundância de Recursos para Tratamento de Informações;
(l) Log;
(m) Atividades de Monitoramento.

Os controles tecnológicos de segurança da informação são medidas implementadas para proteger sistemas, redes e dados contra ameaças cibernéticas. Aqui estão alguns exemplos importantes:

1. **Firewalls**: Dispositivos ou softwares que monitoram e controlam o tráfego de rede com base em regras de segurança predefinidas.
2. **Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS)**: Monitoram a rede ou sistemas para atividades maliciosas ou violações de políticas e podem tomar ações para prevenir

essas ameaças.

3. **Antivírus e Antimalware**: Programas que detectam, previnem e removem softwares maliciosos de computadores e redes.
4. **Criptografia**: Técnica que codifica dados para que apenas pessoas autorizadas possam acessá-los, garantindo a confidencialidade e integridade das informações.
5. **Autenticação Multifator (MFA)**: Requer que os usuários forneçam duas ou mais formas de verificação antes de acessar sistemas ou dados, aumentando a segurança.
6. **Gerenciamento de Identidade e Acesso (IAM)**: Ferramentas e políticas que garantem que as pessoas certas tenham o acesso apropriado aos recursos certos no momento certo.
7. **Soluções de Detecção e Resposta de Endpoint (EDR)**: Monitoram continuamente os endpoints para detectar e responder a atividades suspeitas.

Esses controles são essenciais para proteger a infraestrutura de TI e os dados sensíveis contra uma variedade de ameaças cibernéticas.

Dos controles listados acima:

11 foram classificados como risco leve
00 foram classificados como risco moderado
01 foram classificados como fisco grave
00 foram classificados como risco crítico

Este é o parecer.

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 12:09