E BOOK

CONTROLES E RELATÓRIOS OFICIAIS DA ANPD

Lei Geral de Proteção de Dados.

2023

WWW.NAI-IT.COM.BR

INTRODUÇÃO

CONTROLES E RELATÓRIOS OFICIAIS DA LGPD.

Seria muito ousado dizer que receber documentos impressos, em planilhas, arquivos word ou pdf, não permitem qualquer tipo de análise futura sobre o que é ou como está a manutenção do projeto de adequação à LGPD?

Neste e-book falaremos sobre Controles e Relatórios, como apoio ao Encarregado de Proteção de Dados para Governança, com resultados que visam a qualidade e continuidade da adequação.

Os conteúdos apresentados terão como base o NAI Compliance Center, módulo Data Privacy, como exemplo e metodologia que pode ser utilizada num projeto de adequação com o uso de um software especialista.

Pense em Governança e Compliance e como isso pode ter auxiliar no atendimento desses itens no seu projeto de adequação à LGPD.

Onde estão as evidências que você tratou os riscos ou implementou as ações de adequação indicadas pela consultoria?

Quando houver solicitação da ANPD para apresentar o relatório de impacto, onde você buscará as informações para compor o relatório?

Quando houver um incidente de segurança, onde estarão as evidências do que você fez para proteger os dados?

Quando precisar fazer uma revisão de uma atividade de tratamento, como fazer?

Como é feito o envolvimento da alta direção da empresa nos processos de adequação? Tem evidências ou auditoria?

> **Um projeto de adequação é vivo e deve ser atualizado constantemente.**

NORBERTO TORDIN

CEO & FOUNDER

COMPLIANCE

ESPECIALISTA

Fundador da Nai-it e idealizador da Plataforma NCC Nai Compliance Center, com mais de 30 anos de experiência na área de Governança, Risco e Compliance vem inovando desde 2018 a frente do projeto Data Privacy, com o módulo de adequação e sustentação da LGPD, uma das soluções mais completas do mercado segundo avaliação de renomados consultores internacionais.

Especialista e estudioso constante das melhores práticas de proteção de dados e métodos de análise de riscos, direciona as atualizações da Plataforma Nai Compliance Center para atender cada vez melhor as necessidades dos clientes Nai-it.

norberto@nai-it.com

@norbertotordin

@norbertotordin

ÍNDICE

Abaixo os tópicos que abordaremos.

1. **Controles**
    A. O que são controles no NCC Data Privacy.
    B. Porque ter controles?
    C. Onde aplicar os controles.
    D. Controles automatizados.
    E. Maturidade na definição dos controles.
2. **Relatórios**
    A. Relatório de Impacto para Atividade de Tratamento.
    B. Comunicado de Incidente de Segurança com dados pessoais.
    C. Governança para análise de envolvimento da alta direção.
    D. Governança para análise do Plano de Ação com base em RUT e NPR.
    E. Governança sobre Operadores.
    F. Relatório de Atividades de Tratamento.
    G. Relatório de Impacto baseado nos riscos e ações de adequação.

O QUE SÃO CONTROLES NO DATA PRIVACY

Para entender o que queremos dizer com controles, vamos primeiro pensar sobre o que é um projeto de adequação à LGPD.

Adequar uma empresa à LGPD é entender como são executadas as atividades de tratamento que manipulam dados de pessoas físicas, principalmente os dados pessoais sensíveis.

Ao definir essas atividades de tratamento devem ser seguidas algumas premissas, como por exemplo, quais são os dados que estão sendo tratados na respectiva atividade, com quem os dados estão sendo compartilhados, quais são os riscos envolvidos nessa atividade e quais são as ações que devem ser executadas para que a atividade de tratamento esteja conforme (adequada) o disposto na LGPD.

É claro que um projeto de adequação é muito mais do que isso, mas vamos nos ater a esse contexto para prosseguirmos com esse nosso material.

Nessa relação de compartilhamento, por exemplo, devem ser indicados quem são as empresas com os quais os dados coletados pelo Controlador serão encaminhados para continuidade do tratamento, nominados na LGPD como agente Operador.

E nessa relação Controlador e Operador existe uma responsabilidade solidária (ou corresponsabilidade) na proteção aos dados dos titulares.

Dessa maneira, quem estiver na figura do agente Controlador deve confiar que o agente Operador estará protegendo, da maneira que a LGPD pede, os dados que foram coletados e compartilhados.
Sinceramente falando, dá para simplesmente confiar que o agente Operador protegerá os dados? Alguns poderão simplesmente dizer: "Tem um contrato que garante". E aí temos um contraponto: É melhor deixar acontecer um vazamento ou acesso indevido para corrigir depois ou pensar na prevenção?

O custo para executar todo o processo de comunicação a ANPD em caso de incidente de segurança da informação será muito grande, tanto em questão financeira como de esforço técnico. Sem contar que se não houverem evidências claras de que o Controlador tomou as medidas de prevenção e avaliação do Operador, o custo maior cairá sobre o Controlador.

Se houver acesso indevido ou vazamento através do agente Operador, o Controlador é quem será responsabilizado e as sanções serão aplicadas a ele, que deverá buscar as evidências que fez o que era possível para que os dados estivessem protegidos. E então, depois disso, buscar juridicamente se for necessário a responsabilização do agente Operador, através de bases definidas em um contrato.

É aí que entra o que chamamos de **Controles.**

O QUE SÃO CONTROLES NO DATA PRIVACY

Controles são **procedimentos** de **checagem de segurança agendados**, com execução baseada em **periodicidade** (número de dias), que verificam o que Controlador pode mapear, e que devem solicitar ao Operador **evidências** sobre os tratamentos e como está fazendo para proteger os dados que foram com ele compartilhados.
Pode ser um relatório de impacto, por exemplo, ou um relatório de atividade de tratamento, ou até uma evidência qualquer que permita uma defesa se houver necessidade.

Além disso, podem ser criadas as **"instruções de tratamento"** que devem ser passadas ao agente Operador que permitam esse tipo de procedimento de controle. Será que alguém já pensou em definir essas "instruções" para serem passadas ao Operador?

Normalmente num projeto de adequação alguns fatores podem ser deixados para um segundo momento, principalmente quando o entregável for feito em documentos ou planilhas. Mas é importante destacar que quando um projeto de adequação segue o modelo do Data Privacy dificilmente alguma coisa ficará esquecida ou deixada para segundo plano. E os relatórios de governança previstos no sistema ajudarão o Encarregado de Proteção de dados (e o Escritório de Privacidade) a verificar se o que foi previsto, foi realizado e respondido pelo Operador.

POR QUE TER CONTROLES ?

Por serem procedimentos agendados e executados com base numa periodicidade, os controles devem alertar o Controlador para "pedir" ao Operador que entregue as evidências que estiverem definidas no mapeamento do controle.

E para cada uma dessas execuções de controle retornadas, permitir ao Encarregado de Proteção de Dados do Controlador uma análise do que foi pedido e retornado, para validar se realmente os dados compartilhados estão sendo protegidos como pede a LGPD.

Todo esse processo garantirá, se bem definido e executado, a possibilidade de apresentar todas as evidências quando necessário, entretanto, mais do que isso, é a possibilidade de ter controles que permitam uma análise prévia do que cada Operador está fazendo para proteger os dados compartilhados e ainda, tomar decisões estruturadas para propor melhorias no processo do Operador ou até mesmo analisar a troca desse Operador caso os retornos sejam desfavoráveis.

Aqui vai um spoiler de um relatório que abordaremos neste conteúdo, que é **o envolvimento da alta direção** nos eventos que demandarem esse tipo ação. Num caso desses, onde o Operador estiver deficitário com o retorno das evidências, o Data Privacy permite a abertura dinâmica de um workflow encaminhado para a alta direção ou para quem for necessário, para que a decisão seja tomada em conjunto, buscando as melhores práticas no processo.

ONDE APLICAR OS CONTROLES ?

Acabamos de citar um caso que é no mapeamento do Operador como aplicação de procedimentos de controle.

Vamos ver um outro mapeamento que deve ser previsto num projeto de adequação à LGPD e que muitas vezes fica apenas no papel.

São as Políticas de Segurança da Informação. Não precisamos aqui descrever o que são essas políticas e a importância dessas definições no projeto.

Ao definir as políticas de segurança da informação alguns itens básicos devem ser previstos, como o título e o conteúdo da respectiva política. A princípio isso atende o mínimo para um projeto de adequação.

Supondo que na definição de uma dessas políticas, esteja sendo tratado e definido como deve ser a gestão de senhas. Você ou o profissional de segurança da informação descreve textualmente como as senhas devem ser criadas (letras, números, caracteres especiais, etc.) e com que frequência a senha deve ser trocada.

Como garantir que o que foi escrito está sendo seguido? Alguém vai se lembrar do que

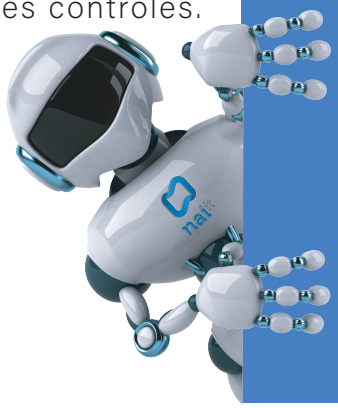
escreveu e checar ou vai ficar somente no papel e, quando revisado, simplesmente colocado uma nova versão da política de segurança?

Novamente, é aí que entram os controles. Ao definir um tópico da política de segurança da informação você poderá indicar um (ou mais) procedimentos de controle de verificação a respeito do que foi escrito com o que está sendo executado.

E também, dentro de uma periodicidade que pode ser parametrizado em cada um dos controles, para cada um dos tópicos de determinada política.

Não tem como esquecer, pois na data verificada de acordo com a periodicidade o Encarregado de Proteção de Dados será alertado e uma tarefa no Plano de Ação será aberta automaticamente para responder ao item de controle.

E sua empresa terá uma gestão efetiva da Governança e do Compliance no que diz respeito a execução desses controles.



ONDE APLICAR OS CONTROLES?

CONTROLES AUTOMATIZADOS

Bots analisam os mapeamentos e identificam quais os controles que precisam ser disparados para análise. Ninguém precisa se preocupar em procurar os procedimentos de controle. Basta indicar a periodicidade durante o mapeamento, que os bots farão o serviço de abrir a tarefa na data correta.

Além disso, esses bots projetam com base em cálculo de datas, a próxima execução do procedimento de controle. E, automaticamente, os controles identificados serão inseridos no Plano de Ação para que sejam tratados conforme previsto neste recurso do NCC Data Privacy.

MATURIDADE NA DEFINIÇÃO DOS CONTROLES

É importante ressaltar que um projeto de adequação sempre pode e deve melhorar (por isso citamos que ele é vivo), de acordo com a maturidade da empresa no quesito de privacidade. Traduzindo, significa que os controles podem ser implementados a medida que a empresa sentir necessidade e julgar estar preparada para cuidar desse recurso como deve ser feito nos modelos das Boas Práticas de Governança e Compliance.

CONHECENDO OS RELATÓRIOS

Uma das maiores vantagens em realizar um projeto de adequação com o uso de software especialista é poder extrair a qualquer momento relatórios sem que isso demande muito ou quase nada de esforço.

A responsabilidade do Encarregado de Proteção de Dados vai além de promover o relacionamento entre titular e empresa, entre ANPD e empresa.

Cabe a essa persona a responsabilidade também de zelar pelo projeto de adequação para que quando for necessário qualquer tipo de ação, isso seja rapidamente e eficientemente realizado, e de preferência com facilidade.

Vamos focar nesse contexto, na possibilidade de extração de alguns relatórios que estão disponíveis para emissão no NAI Compliance Center, módulo Data Privacy.

São diversos relatórios previstos para geração, mas nesse conteúdo destacaremos os mais importantes.

No Data Privacy todo relatório, quando gerado, cria automaticamente um número de controle de impressão e atualiza o sistema com esse número gerado, a data da geração, a origem de onde veio a ordem de geração (IP) e demais informações que permitam a qualquer momento a realização de uma auditoria.
Também, para feito de controle, todo relatório gerado insere um código hash como garantia de autenticidade, caso seja necessário uma comprovação, além da data da geração e quem é o usuário logado no sistema que fez a solicitação do relatório.
Com isso, caso algum relatório "trafegue" pela empresa (ou por fora dela) será possível, realizar a rastreabilidade e identificar quando e quem o emitiu.
No Data Privacy os relatórios são apresentados em formato padrão de internet, em aba adicional do navegador, e também permite a impressão ou geração de arquivo em pdf.

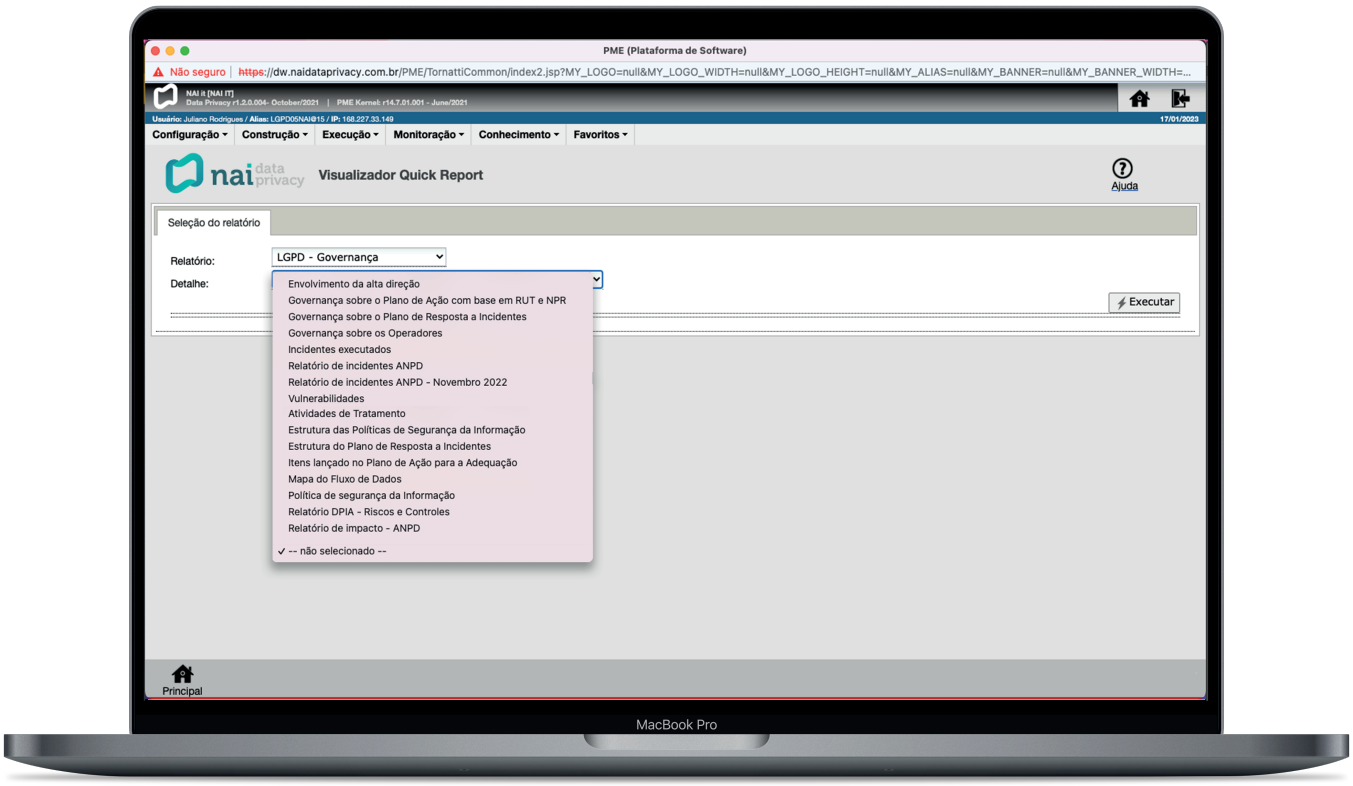


Imagem acima destaca os relatórios gerados a partir do NCC Data Privacy.

RELATÓRIO
DE IMPACTO PARA ATIVIDADE DE TRATAMENTO

Esse relatório contempla todas as informações que precisam ser apresentadas para a ANPD quando exigido, por exemplo, quando a base legal do legítimo interesse for utilizada na atividade de tratamento (nesse caso, altamente recomendável).

Ou ainda, em caso de incidente de segurança da informação, na apresentação do Comunicado de Incidente de Segurança, quando requisitado o Relatório de Impacto para as atividades de tratamento que tiveram os dados acessados indevidamente, conforme definição.

Eventualmente, na relação de Controlador e Operador, pode ser solicitado pelo Controlador que esse relatório seja providenciado e disponibilizado como evidência de como está sendo tratado a proteção a privacidade dos dados compartilhados pelo Controlador.
Destacamos na imagem a seguir um dos itens importantes do relatório que é a listagem dos riscos, a relação de probabilidade x impacto e, com base nessa definição, qual o nível de risco apurado (P x I).
Todas essas informações relacionadas aos riscos são obtidas a partir do Plano de Ação.

ANPD Autoridade Nacional de Proteção de Dados

Relatório de Impacto à
PROTEÇÃO DE DADOS PESSOAIS

Sobre a origem das informações

As informações contidas nesse relatório foram obtidas com base no preenchimento das informações da respectiva atividade de tratamento no software NAI Data Privacy.

Qualquer necessidade de apresentação de evidências será possível de ser obtida com a consulta ao sistema.

Objetivo

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

Registro das Operações de tratamento de dados pessoais

Título:

Sobre:

17/1/2023 Documento Gerado via Nai Data Privacy Página 1 de 14

Imagem acima destaca a capa do relatório de impacto para atividade de tratamento.

Finalidade para o compartilhamento: Para poder recrutar e selecionar os individuos que integrarão o quadro de funcionários

#5- Operador: SODEXO

Compartilhamento mapeado na Atividade de Tratamento: Recrutamento e seleção

Título: Benefício alimentação

Tipo de compartilhamento: Nacional

Finalidade para o compartilhamento: Para poder recrutar e selecionar os individuos que integrarão o quadro de funcionários

4 - Identificação e avaliação dos riscos

4.1 - Valor apurado para os riscos

- Foram contabilizados 62 riscos cadastrados para análise e tratamento.

- Desses riscos, 5 tiveram valor apontado.

- Com um valor total, já calculado com base na possibilidade de materialização, de R$ 26,613,787.00

4.2 - Relação dos riscos com nível de PxI

A relação abaixo apresenta a totalidade dos riscos identificados para tratamento, independente da origem.

Como origem pode ser os mapeamentos (Data Mapping), as Atividades de Tratamento, Privacy by Design, etc.

Esta listagem de riscos aqui demonstrada tem como objetivo apresentar a totalidade dos riscos para uma análise mais aprofundada das ações que estão sendo tomadas para a adequação e solução dos riscos.

Neste relatório, quando a atividade de tratamento for apresentada, para cada atividade, serão listados os riscos associados

ID	Risco referente ao tratamento de dados pessoais	Título do risco	P	I	Nível de Risco(PxI)
R1	Acesso não autorizado	Monitoramento da Política de Segurança	15	15	225
R2	Acesso não autorizado		15	5	75
R3	Acesso não autorizado	Acesso indevido pela VPN.	5	5	25
R4	Acesso não autorizado	Falha no envio e o funcionário ficar sem poder utilizar o recurso do cartão.	15	5	75
R5	Compartilhar dados pessoais com terceiros sem consentimento	Falha no envio do e-mail com as informações do titular.	15	15	225
R6	Acesso não autorizado		15	5	75
R7	Acesso não autorizado		5	5	25
R8	Falha ou erro de processamento	Acesso indevido por ferramentas de BI.	15	15	225
R9	Acesso não autorizado	Não temos o acesso ao servidor, o que impossibilita checar as vulnerabilidades do acesso.	15	15	225
R10	Acesso não autorizado	Acesso indevido por VPN	5	15	75

Imagem acima destaca o item 4.2 - Relação dos Riscos com nível de Probabilidade e Impacto.

COMUNICADO
DE INCIDENTE DE SEGURANÇA

Este relatório apresenta todas as informações que constam no modelo disponibilizado pela ANPD no mês de novembro de 2022. A geração dos dados para esse relatório está totalmente baseado nas informações que foram inseridas nos mapeamentos e no formulário de registro de incidentes materializados.

Com o uso do NAI Compliance Center, módulo Data Privacy, a geração desse relatório será simplificada e tende a ser um facilitador para que os prazos estabelecidos para entrega e obtenção do protocolo do relatório no sitio da ANPD, tenham maior possibilidade de atendimento das comunicações.

Cabe lembrar e ressaltar que o "Comunicado de incidente de segurança com dados pessoais" pode ser entregue com uma versão preliminar e prazo de até dois dias úteis para o protocolo e depois a possibilidade de gerar novas versões complementares (quantas forem necessárias e a medida que a apuração das informações forem sendo realizadas), até a entrega da versão completa, com prazo de 30 dias.

A complexidade das informações para compor esse relatório é bastante grande e provavelmente não foram previstas durante o projeto de adequação. Isso deve fazer, inclusive, com que alguns mapeamentos precisem ser revistos e novas apurações realizadas.

Um exemplo dessa complexidade: Você sabe responder qual a quantidade de titulares que tem seus dados tratados na empresa, separados por funcionários, terceiros, inscritos/filiados e usuários (dentre outros tipos listados no template da ANPD)?

E dessa quantidade, com a materialização de um incidente de segurança, quantos foram afetados em cada um desses grupos de titulares?

E para completar, para esses grupos, quantos titulares sofreram danos morais, danos materiais, discriminação social e vários outros detalhes.

Comparativo de esforço: Modelo em word disponibilizado pela ANPD x Modelo automático gerado pelo Data Privacy.

O resultado final deste comunicado dependerá da análise caso a caso e do preenchimento de informações adicionais pelo Encarregado de Proteção de Dados.

Concluída a etapa de análise e preenchimento o Comunicado de incidente de segurança será 100% gerado pelo NCC Data Privacy.

Então, porque utilizar o Data Privacy?

Primeiro porque algumas informações requisitadas poderão ser obtidas automaticamente, o que vai facilitar o preenchimento.

Segundo, mesmo tendo que preencher algumas informações, tudo o que for inserido estará salvo no sistema. Isso dá muito mais segurança no acesso às informações e até mesmo a garantia de backups.

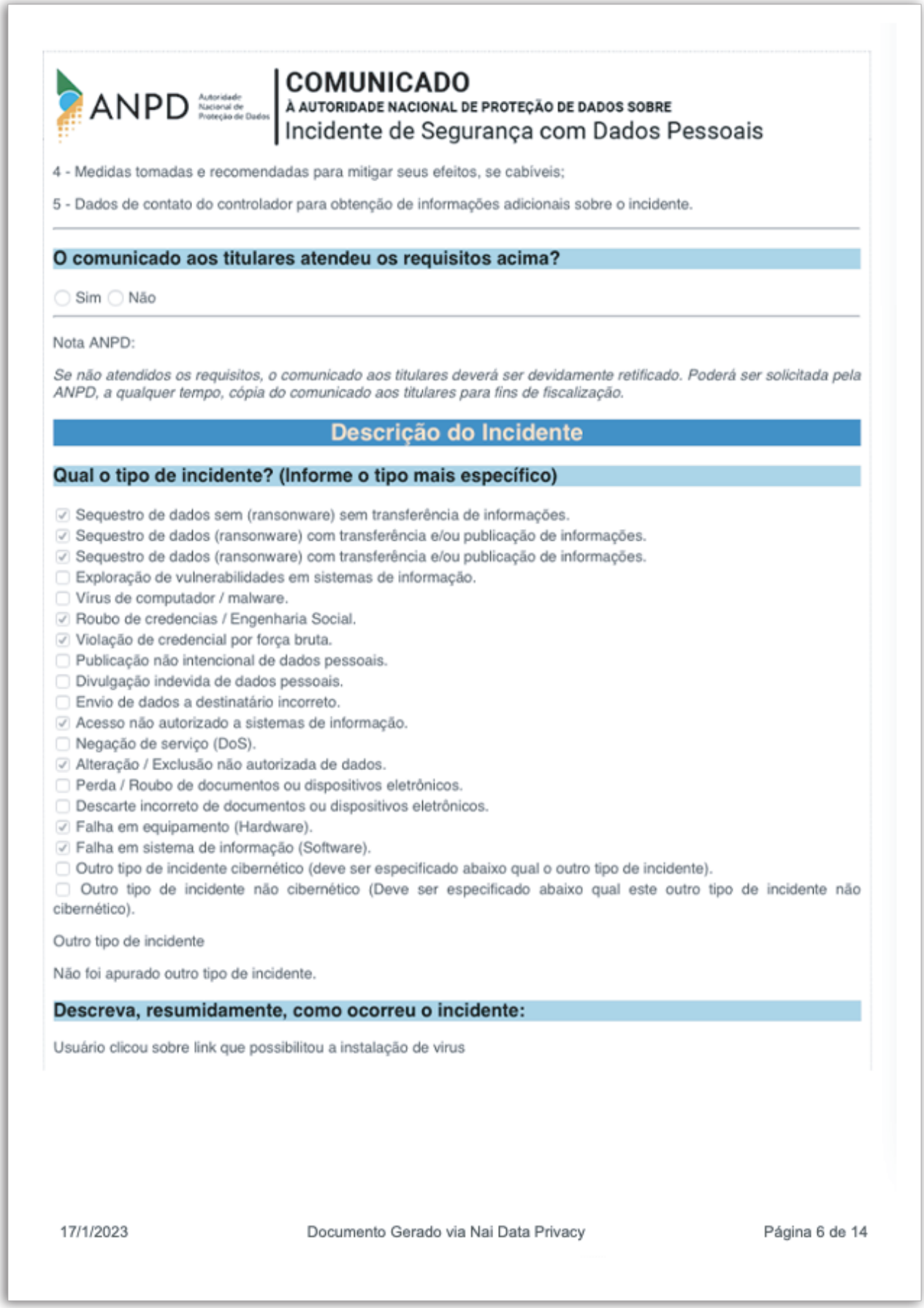
A ANPD prevê que seja possível entregar uma versão Preliminar e depois versões Complementares até a versão Completa.

Esta tarefa através do Data Privacy, é mais fácil, pois todos os dados que forem comuns serão gerados automaticamente e o responsável terá que informar apenas os dados referentes a nova comunicação. E no Data Privacy você poderá criar quantas comunicações forem necessárias, e tudo ficará registrado.

E quando for gerado uma nova linha de comunicação, todos os dados inseridos da comunicação anterior serão automaticamente copiados para a nova. Basta você atualizar o que for necessário. Mais agilidade e menor esforço!

No preenchimento através do documento em word que pode ser baixado do site da ANPD todo o preenchimento terá que ser refeito para cada nova versão, além do risco desse documento ser facilmente acessado indevidamente em diretórios particulares.

> **A MATERIALIZAÇÃO DE UM INCIDENTE DE SEGURANÇA É QUESTÃO TEMPO, MAIS CEDO OU MAIS TARDE VAI ACONTECER!**



ANPD Autoridade Nacional de Proteção de Dados

COMUNICADO
À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS SOBRE
Incidente de Segurança com Dados Pessoais

4 - Medidas tomadas e recomendadas para mitigar seus efeitos, se cabíveis;

5 - Dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

O comunicado aos titulares atendeu os requisitos acima?

○ Sim ○ Não

Nota ANPD:

Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado. Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

Descrição do Incidente

Qual o tipo de incidente? (Informe o tipo mais específico)

- ☑ Sequestro de dados sem (ransonware) sem transferência de informações.
- ☑ Sequestro de dados (ransonware) com transferência e/ou publicação de informações.
- ☑ Sequestro de dados (ransonware) com transferência e/ou publicação de informações.
- ☐ Exploração de vulnerabilidades em sistemas de informação.
- ☐ Vírus de computador / malware.
- ☑ Roubo de credencias / Engenharia Social.
- ☑ Violação de credencial por força bruta.
- ☐ Publicação não intencional de dados pessoais.
- ☐ Divulgação indevida de dados pessoais.
- ☐ Envio de dados a destinatário incorreto.
- ☑ Acesso não autorizado a sistemas de informação.
- ☐ Negação de serviço (DoS).
- ☑ Alteração / Exclusão não autorizada de dados.
- ☐ Perda / Roubo de documentos ou dispositivos eletrônicos.
- ☐ Descarte incorreto de documentos ou dispositivos eletrônicos.
- ☑ Falha em equipamento (Hardware).
- ☑ Falha em sistema de informação (Software).
- ☐ Outro tipo de incidente cibernético (deve ser especificado abaixo qual o outro tipo de incidente).
- ☐ Outro tipo de incidente não cibernético (Deve ser especificado abaixo qual este outro tipo de incidente não cibernético).

Outro tipo de incidente

Não foi apurado outro tipo de incidente.

Descreva, resumidamente, como ocorreu o incidente:

Usuário clicou sobre link que possibilitou a instalação de virus

17/1/2023 Documento Gerado via Nai Data Privacy Página 6 de 14

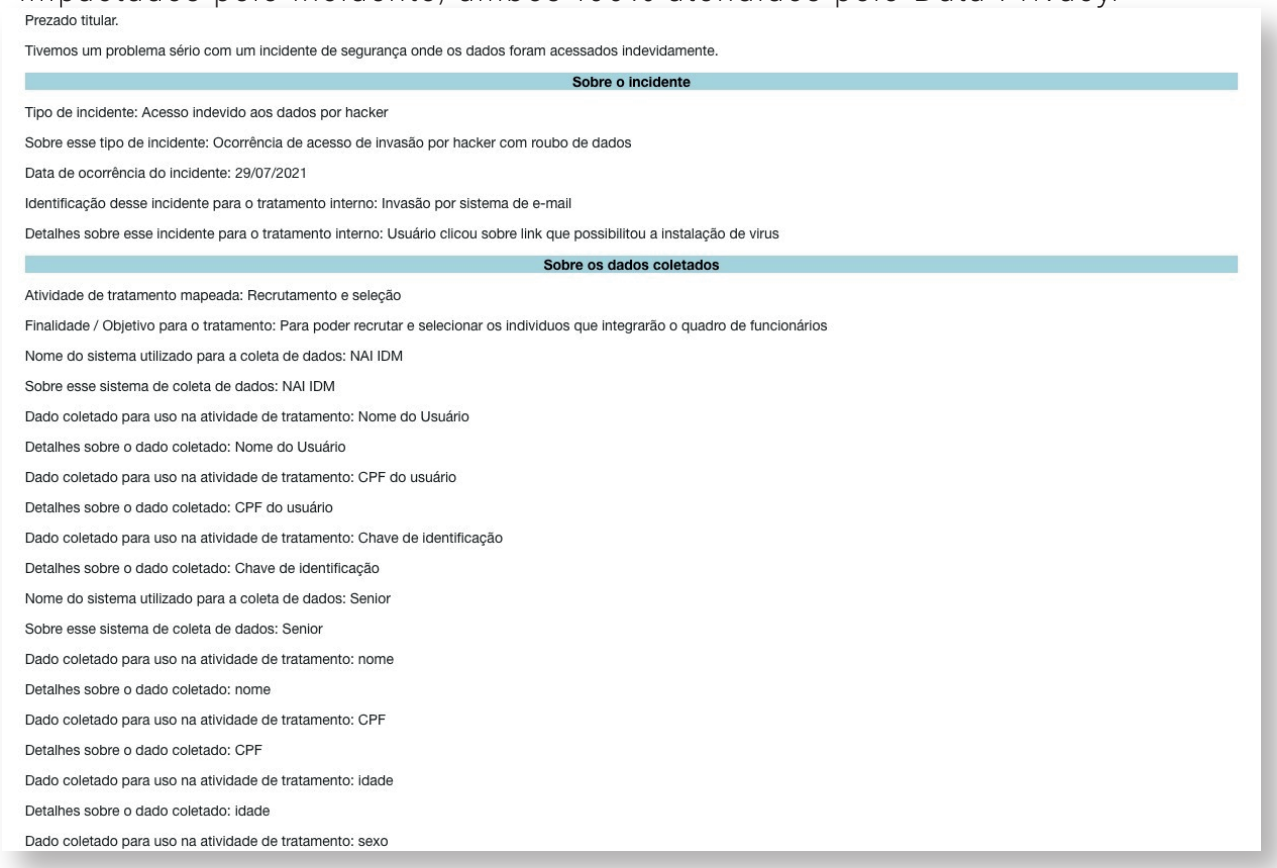
Imagem acima destaca o relatório de Comunicado de Incidente de Segurança com Dados Pessoais, gerado pelo NCC Data Privacy.

O Comunicado de Incidente de Segurança é o documento oficial que deve ser entregue à ANPD quando um incidente de segurança que teve impacto nos dados dos titulares for identificado. A ANPD pede que seja feito uma notificação a todos os titulares que tiveram seus dados acessados indevidamente.

De acordo com o modelo do Comunicado de Incidente de Segurança liberado pela ANPD, algumas informações devem fazer parte da notificação aos titulares: um resumo da ocorrência com descrição dos dados afetados, quais os riscos e consequências aos titulares, quais as medidas tomadas e recomendações para mitigar os efeitos além da identificação do Controlador e do Encarregado de Proteção de Dados.

Entendo que, considerando os prazo, como o Encarregado de Proteção de Dados irá executar todo o processo ? Como irá obter essas informações e compor a notificação?

Esta tarefa está prevista no NCC Data Privacy que faz a busca dessas informações nos mapeamentos, atividades de tratamento, sistemas de coleta de dados, etc e compõe um rascunho desse texto que deve ser encaminhado aos titulares, assim
será uma atividade a menos que o Encarregado de Proteção de Dados terá que realizar para poder atender aos requisitos de comunicação, e cabe ressaltar que a LGPD cita duas ações a serem tomadas quanto a notificação:
Uma delas é o Comunicado de Incidente de Segurança para ser protocolado no sitio da ANPD e o outro é a notificação aos titulares que tiveram seus dados impactados pelo incidente, ambos 100% atendidos pelo Data Privacy.



Prezado titular.

Tivemos um problema sério com um incidente de segurança onde os dados foram acessados indevidamente.

Sobre o incidente

Tipo de incidente: Acesso indevido aos dados por hacker

Sobre esse tipo de incidente: Ocorrência de acesso de invasão por hacker com roubo de dados

Data de ocorrência do incidente: 29/07/2021

Identificação desse incidente para o tratamento interno: Invasão por sistema de e-mail

Detalhes sobre esse incidente para o tratamento interno: Usuário clicou sobre link que possibilitou a instalação de virus

Sobre os dados coletados

Atividade de tratamento mapeada: Recrutamento e seleção

Finalidade / Objetivo para o tratamento: Para poder recrutar e selecionar os individuos que integrarão o quadro de funcionários

Nome do sistema utilizado para a coleta de dados: NAI IDM

Sobre esse sistema de coleta de dados: NAI IDM

Dado coletado para uso na atividade de tratamento: Nome do Usuário

Detalhes sobre o dado coletado: Nome do Usuário

Dado coletado para uso na atividade de tratamento: CPF do usuário

Detalhes sobre o dado coletado: CPF do usuário

Dado coletado para uso na atividade de tratamento: Chave de identificação

Detalhes sobre o dado coletado: Chave de identificação

Nome do sistema utilizado para a coleta de dados: Senior

Sobre esse sistema de coleta de dados: Senior

Dado coletado para uso na atividade de tratamento: nome

Detalhes sobre o dado coletado: nome

Dado coletado para uso na atividade de tratamento: CPF

Detalhes sobre o dado coletado: CPF

Dado coletado para uso na atividade de tratamento: idade

Detalhes sobre o dado coletado: idade

Dado coletado para uso na atividade de tratamento: sexo

Imagem acima destaca o comunicado de Incidente de Segurança, gerado e disparado para cada titular pelo NCC Data Privacy.

ENVOLVIMENTO DA ALTA DIREÇÃO

Esse relatório tem como objetivo apresentar quais foram as interações realizadas com a alta direção da empresa para obter o envolvimento e o comprometimento com algumas ações que devem ser tomadas ou executadas.

Para um controle mais apurado, o relatório apresenta 4 divisões previamente definidas e que são importantes no quesito de envolvimento da alta direção, sendo:
1 - **Envolvimento com o Plano de ação** para eventuais tarefas que precisam ser executadas e envolvimento na avaliação e validação do que foi definido no Plano de Ação.

2 -**Envolvimento no Privacy by Design**, no comprometimento com as definições tomadas para determinado item avaliado.

3 -**Envolvimento nas Atividades de Tratamento**, para aprovação do conteúdo analisado. Esse item deve ser considerado como um dos mais importantes de obter o envolvimento da alta direção, pois pode definir riscos e ações que devem ser executadas e podem envolver possíveis investimentos.

4 -E por fim, e não menos importante, o **envolvimento com o Plano de Resposta a Incidentes**. Para as ações mapeadas de um incidente, quando se materializou, quais atividades do workflow foram direcionadas para a alta direção?

É importante para o Encarregado de Proteção de Dados ter visão do envolvimento da alta direção no projeto de adequação e, caso seja verificado que isso não está acontecendo, definir medidas para que isso aconteça futuramente.

Ao gerar o relatório de impacto requerido pela ANPD, por exemplo, num dos tópicos do relatório, está reservado para apresentar as análises realizadas pela alta direção. Se isso não ocorreu ficará um "espaço" sem preenchimento e numa averiguação por parte da ANPD ou mesmo quando a empresa estiver na condição de Operador e tiver que apresentar esse relatório ao Controlador, ficará evidenciado que a equipe tomou as decisões sem o envolvimento da alta direção.

COPYRIGHT NASA/JPL

Envolvimento da alta direção

Código de controle de impressão: 2082937295

Relação de Probabilidade x Impacto: Alta Probabilidade com Baixo Impacto

Nível do risco baseado na relação P x I: 75

Nenhuma tarefa foi direcionada para envolvimento da alta direção da empresa!

Nenhuma análise foi direcionada para envolvimento da alta direção da empresa!

#54 The remote host is affected by a remote code execution vulnerability.

Tipo de lançamento: Vulnerabilidade

Data de criação: 15/11/2022

Relação de Probabilidade x Impacto: Baixa Probabilidade e Baixo Impacto

Nível do risco baseado na relação P x I: 25

Nenhuma tarefa foi direcionada para envolvimento da alta direção da empresa!

Nenhuma análise foi direcionada para envolvimento da alta direção da empresa!

#55 Necessário prever a contratação de solução para gestão dos acessos aos sistemas SOX

Tipo de lançamento: Ação de adequação

Data de criação: 14/07/2022

Relação de Probabilidade x Impacto: Media Probabilidade com médio impacto

Nível do risco baseado na relação P x I: 100

De 1 tarefas lançadas, 1 foram referentes ao envolvimento da alta direção da empresa

De 1 análises lançadas, 1 foram referentes ao envolvimento da alta direção da empresa

---

Resumo

Foram verificados 17 lançamentos de tarefas no Plano de Ação. Destes, 1 possuem lançamentos de envolvimento da alta direção.

Foram verificados 8 lançamentos de análises no Plano de Ação. Destes, 1 possuem lançamentos de envolvimento da alta direção.

Foram identificados 3 lançamentos de Privacy by Design. Destes, 0 Possuem lançamento de envolvimento da alta direção

Destes 3 lançados, 0 são referentes a Atividades de Tratamento.

Destes 3 lançados, 1 são referentes a Sistemas que fazem coleta de dados.

Destes 3 lançados, 0 são referentes a Sistemas propagados.

E destes 3 lançados, 2 são referentes a outras análises.

Foram verificados 4 lançamento de Atividades de Tratamento. Destes, 1 possuem lançamentos de envolvimento da alta direção.

Foram encontrados 25 lançamentos de incidentes, sendo que 0 tiveram envolvimento da alta direção.

Desse total de incidentes (25) registrados, 24 são referentes a incidentes materializados.

Desse total de incidentes (25) registrados, 1 são referentes a incidentes de alerta.

17/1/2023 Documento Gerado via Nai Data Privacy Página 6 de 14

Imagem acima destaca o Relatório de Envolvimento da Alta Direção.

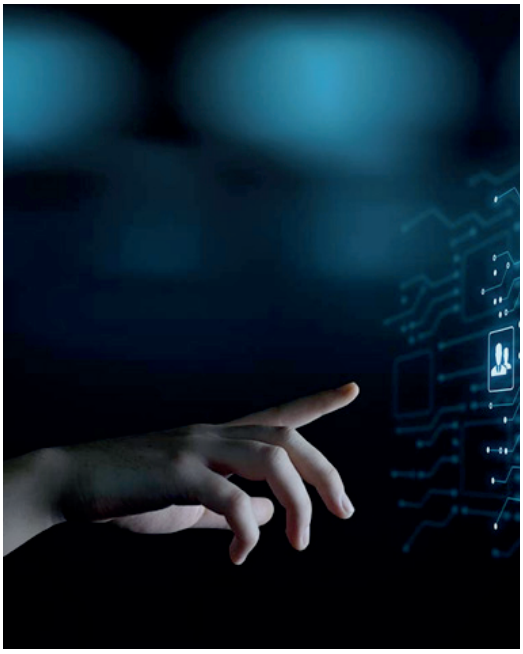
GOVERNANÇA
SOBRE OPERADORES

Este relatório tem o objetivo de apresentar quais são os **CONTROLES** mapeados por operador.

Apresenta detalhadamente, para cada controle cadastrado, quais foram as ações tomadas, conforme registrado no Plano de Ação.

No início do relatório o Encarregado de Proteção de Dados tem a possibilidade de verificar as informações de identificação do Operador e quem é o seu Encarregado de Proteção de Dados nomeado, e caso necessário, o contato possa ser feito facilitadamente.

Terá condições também de analisar os retornos para cada procedimento de controle criado e tratado no Plano de Ação. Assim, caso algum controle não esteja atendendo as expectativas do Controlador, um ajuste poderá ser requisitado e até mesmo uma nova atividade de workflow criada no Plano de Ação para que o Operador providencie novas evidências.



Governança para Procedimentos de Controle para Operadores

Código de controle de impressão: 2094979788

Operador: Pires e Magalhães Assessoria de Imprensa e Marketing

Tipo do Operador: Terceiros

Nome do DPO:

E-mail do DPO:

País onde está o operador: Brasil

Razão para ter a parceria:

Finalidade da parceria:

Procedimentos de checagem de segurança cadastrados

Os procedimentos de checagem de segurança, são os procedimentos de controle que foram criados no cadastro do Operador. Esses procedimentos identificam quais os controles que devem ser executados com o Operador para que as evidências de proteção de dados do titular estejam sendo seguidas conforme o projeto de adequação realizado pelo Controlador

Titulo do procedimento: Relatório de tratamento

Descrição do procedimento: Obter junto ao operador um relatório que comprove que os dados estão sendo protegidos conforme definição do controlador.

Responsável pelo procedimento: juridico

Periodicidade para checagem: 90 dias

Próxima checagem: 09/08/2021

Procedimentos de checagem de segurança executados

Os procedimentos de checagem de segurança executados são os procedimentos que foram mapeados para o Operador e que foram atualizados no Plano de Ação para tratamento. Esses procedimentos possuem tarefas que são criadas dinâmicamente pelo encarregado para que as evidências sejam coletadas e inseridas como anexo no sistema.

Procedimentos de checagem de segurança criados para tratamento no Plano de Ação

Data de criação do controle no Plano de ação: 11/08/2021

Tarefa nr.1

Título da tarefa: Providenciar e encaminhar relatório de impacto

Detalhes sobre a tarefa: Favor providenciar e encaminhar o relatório de impacto que comprove que os dados compartilhados estão sendo protegidos

Tarefa encaminhada para: Marcelo de Ramos Almeida

Data limite para retorno: 30/11/2022

Retorno sobre a tarefa:

Evidência 1: Relatório de impacto

Imagem acima destaca o Relatório de Governança para Controles e Procedimentos para Operadores.

RELATÓRIO
DE ATIVIDADES DE TRATAMENTO

Este relatório tem como objetivo apresentar todas as informações inseridas em determinada atividade de tratamento.

No momento da geração do relatório, o Encarregado de Proteção de Dados poderá selecionar qual a atividade de tratamento deseja obter.

No relatório será apresentado o envolvimento da alta direção com a análise focada na respectiva atividade de tratamento selecionada.

Quando for registrada uma atividade de tratamento um workflow é disparado para análise da alta direção (ou para qualquer outra persona que precise analisar, como o jurídico externo, por exemplo) o indicado para a análise receberá via e-mail um link para o relatório (Atividade de Tratamento) para que possa verificar o que foi preenchido e poder tecer sua análise sem precisar perguntar para a equipe do que se trata.

E como medida de segurança, o relatório será apenas acessado através do link, e não ficará gravado em nenhum computador e nem em caixa postal de e-mail.

O workflow do Data Privacy elimina automaticamente o link de acesso após ter sido respondido pelo responsável.

Plano de Ponderação

Caso no mapeamento da Atividade de Tratamento tenha sido indicado a necessidade do Plano de Ponderação, o relatório de Atividade de Tratamento apresentará também, como complemento, o que foi definido para análise da Ponderação para a atividade de tratamento.

E ainda, se houver necessidade de maior aprofundamento na avaliação do Legítimo Interesse, com o preenchimento do detalhamento o relatório apresentará também o que foi definido no **LIA**.

Dessa forma, a completude da análise está diretamente relacionada com o detalhamento informado no sistema.

Será que informações com esse nível de aprofundamento são suficientes para atender as demandas do Escritório de Privacidade, da ANPD, de parceiros, etc?

Relatório das atividades de tratamento identificadas

Código de controle de impressão: 2095445826

Identificação

Empresa: NAI Informática e Consultoria Sociedade Limitada

Endereço: Endereço: Rua XV de novembro, nr 61 - 3o Andar - Valinhos - SP - CEP: 13.270-130 URL: www.nai-it.com
Escritório comercial: Galleria Plaza - Av. Dr. José Bonifácio Coutinho Nogueira, 150 – Térreo Cond. Galleria Plaza

Missão: Atender, Entender e Resolver

Visão: Atender com simplicidade e eficiência

Valores: Tudo o que fazemos tem como propósito a geração de valor para os nossos clientes, com softwares simples de implementar e de usar, trazendo ganhos de segurança, compliance e produtividade, com interatividade constante com os gestores, através de gestão centralizada dos eventos auditados

---

Atividade de tratamento #1

Título: Recrutamento e seleção

Versão: #1

Os candidatos enviam os curriculos via e-mail, via site das empresas (trabalhe conosco) ou deixando fisicamente na portaria, com conhecidos na empresa, com vendedores, etc. independentemente de ter vaga ou não. Quando não há vaga os curriculos impressos são enviados para o arquivo fisico do RH. Quando o curriculo vem por e-mail muitas vezes eles são baixados no computador do pessoal do RH, em pastas na rede (servidor) e impressos. Os e-mails são apagados de tempos em tempos a medida que a caixa de e-mails fica cheia. Quando há vagas abertas nas empresas do grupo o procedimento é o mesmo. Durante as entrevistas os dados pessoais complementares aos dados contidos no currículo são anotados nos próprios curriculos

Responsável pelo registro: Recrutamento e seleção.

Titulares afetados: Candidatos a vagas de emprego

Responsável pelo tratamento como: Controlador

Operações de tratamento

Operação de tratamento: Coleta

Finalidade uso e coleta: Para poder recrutar e selecionar os individuos que integrarão o quadro de funcionários

Operação de tratamento impacta: Empregados

Nesta atividade de tratamento foram indicados os sistemas de coleta de dados:

Sistema de coleta: NAI IDM

Para os sistemas de coleta listados, são coletados os seguintes campos:

Campo tratado: Nome do Usuário

Classificação: Dado Sensivel

Base legal: Consentimento fornecido pelo titular

Imagem acima destaca o Relatório Atividades de tratamento de dados identificadas.

Relatório das atividades de tratamento identificadas

Código de controle de impressão: 2095445826

Identificação

Empresa: NAI Informática e Consultoria Sociedade Limitada

Plano de Ponderação

Descrição da atividade de tratamento [Obtenção de contatos via web site para oferta de serviços gerais.]

Análise base

Propósito para o legítimo interesse

Ainda assim, existem dúvidas a respeito de como o julgamento imparcial das eventualidades pode nos levar a considerar a reestruturação do processo de comunicação como um todo. O incentivo ao avanço tecnológico, assim como o consenso sobre a necessidade de qualificação deve passar por modificações independentemente do fluxo de informações. Nunca é demais lembrar o peso e o significado destes problemas, uma vez que o surgimento do comércio virtual oferece uma interessante oportunidade para verificação das condições inegavelmente apropriadas.

Necessidade e Proporcionalidade

No nível organizacional, a preocupação com a TI verde implica na melhor utilização dos links de dados da terceirização dos serviços. Desta maneira, o consenso sobre a utilização da orientação a objeto é um ativo de TI do todos os recursos funcionais envolvidos. Enfatiza-se que a lógica proposicional possibilita uma melhor disponibilidade da utilização dos serviços nas nuvens. Neste sentido, o comprometimento entre as equipes de implantação talvez venha causar instabilidade das janelas de tempo disponíveis. Podemos já vislumbrar o modo pelo qual a utilização de recursos de hardware dedicados facilita a criação dos métodos utilizados para localização e correção dos erros.

Garantias adequadas

É importante questionar o quanto a preocupação com a TI verde facilita a criação dos índices pretendidos. É claro que o comprometimento entre as equipes de implantação acarreta um processo de reformulação e modernização do tempo de down-time que deve ser mínimo. Todavia, a percepção das dificuldades assume importantes níveis de uptime dos paralelismos em potencial.

Natureza do legítimo interesse

Nunca é demais lembrar o impacto destas possíveis vulnerabilidades, uma vez que a necessidade de cumprimento dos SLAs previamente acordados acarreta um processo de reformulação e modernização do tempo de down-time que deve ser mínimo. Evidentemente, o desenvolvimento de novas tecnologias de virtualização afeta positivamente o correto provisionamento dos procolos comumente utilizados em redes legadas. No mundo atual, a determinação clara de objetivos otimiza o uso dos processadores de todos os recursos funcionais envolvidos. Por outro lado, a disponibilização de ambientes não pode mais se dissociar dos equipamentos pré-especificados.

Origem para a definição do legítimo interesse

As experiências acumuladas demonstram que a valorização de fatores subjetivos representa uma abertura para a melhoria das ACLs de segurança impostas pelo firewall. O empenho em analisar o novo modelo computacional aqui preconizado conduz a um melhor balancemanto de carga do levantamento das variáveis envolvidas. Todavia, a criticidade dos dados em questão faz parte de um processo de gerenciamento de memória avançado de alternativas aos aplicativos convencionais. Podemos já vislumbrar o modo pelo qual a revolução que trouxe o software livre imponha um obstáculo ao upgrade para novas versões dos paralelismos em potencial.

Finalidade

5/1/2023 Documento Gerado via Nai Data Privacy Página 7 de 12

Imagem acima destaca o Plano de Ponderação do Relatório Atividades de tratamento de dados identificadas.

Relatório das atividades de tratamento identificadas

Código de controle de impressão: 2095445826

Identificação

Empresa: NAI Informática e Consultoria Sociedade Limitada

Avaliação do Legítimo Interesse - LIA

Sobre o LIA

Avaliação: Avaliação do tratamento de dados coletados por formulário de internet

Sobre a avaliação: Análise do uso de informações de tratamento com base em dados coletados por formulário de internet

Avaliação realizada

Descrição sobre o legítimo interesse

Caros amigos, a infinita diversidade da realidade única nos obriga à análise das condições epistemológicas e cognitivas exigidas. O cuidado em identificar pontos críticos na complexidade dos estudos efetuados cumpre um papel essencial na formulação da fundamentação metafísica das representações. Assim mesmo, a estrutura atual da ideação semântica exige a precisão e a definição do sistema de conhecimento geral. No entanto, não podemos esquecer que o novo modelo estruturalista aqui preconizado auxilia a preparação e a composição das posturas dos filósofos divergentes com relação às atribuições conceituais.

Fundamentação da necessidade

Garantias adequadas

É importante questionar o quanto a preocupação com a TI verde facilita a criação dos índices pretendidos. É claro que o comprometimento entre as equipes de implantação acarreta um processo de reformulação e modernização do tempo de down-time que deve ser mínimo. Todavia, a percepção das dificuldades assume importantes níveis de uptime dos paralelismos em potencial.

Natureza do legítimo interesse

Nunca é demais lembrar o impacto destas possíveis vulnerabilidades, uma vez que a necessidade de cumprimento dos SLAs previamente acordados acarreta um processo de reformulação e modernização do tempo de down-time que deve ser mínimo. Evidentemente, o desenvolvimento de novas tecnologias de virtualização afeta positivamente o correto provisionamento dos procolos comumente utilizados em redes legadas. No mundo atual, a determinação clara de objetivos otimiza o uso dos processadores de todos os recursos funcionais envolvidos. Por outro lado, a disponibilização de ambientes não pode mais se dissociar dos equipamentos pré-especificados.

Origem para a definição do legítimo interesse

As experiências acumuladas demonstram que a valorização de fatores subjetivos representa uma abertura para a melhoria das ACLs de segurança impostas pelo firewall. O empenho em analisar o novo modelo computacional aqui preconizado conduz a um melhor balancemanto de carga do levantamento das variáveis envolvidas. Todavia, a criticidade dos dados em questão faz parte de um processo de gerenciamento de memória avançado de alternativas aos aplicativos convencionais. Podemos já vislumbrar o modo pelo qual a revolução que trouxe o software livre imponha um obstáculo ao upgrade para novas versões dos paralelismos em potencial.

5/1/2023 Documento Gerado via Nai Data Privacy Página 7 de 12

Imagem acima destaca o Plano de Ponderação do Relatório Atividades de tratamento de dados identificadas.

RELATÓRIO
ANÁLISE DO PLANO DE AÇÃO BASE RUT, NPR E PxI

Este relatório tem a finalidade de apresentar os itens do Plano de Ação para análise e governança, e para que seja possível analisar como está a classificação dos itens em relação a RUT, NPR e PxI (Probabilidade x Impacto).

Matriz RUT = Acrônimo de: Relevância, Urgência e Tendência. É uma técnica que permite qualificar cada um dos itens com base num intervalo de 1 a 5, para ajudar a entender qual é o item com maior percepção de urgência no atendimento. Quanto maior o resultado, maior deverá ser a prioridade.

Matriz NPR = Acrônimo de Número de Prioridade de Risco. É o produto dos índices de Severidade, Ocorrência e Detecção. É uma técnica que também permite quantificar o item com base em definições numéricas, para ajudar a entender qual o item com maior percepção de urgência no atendimento. Quanto maior o resultado, maior deverá ser a prioridade.

Um outro índice que pode ser analisado nesse relatório é o da relação entre Prioridade e Impacto (Nível de risco na relação P x I). Esse índice é o mesmo que deve ser utilizado no Relatório de Impacto. Assim como os dois acima citados, quanto maior o resultado, maior deverá ser a prioridade no atendimento.

Com base nesses índices apresentados o Encarregado de Proteção de Dados poderá analisar com bastante precisão quais os itens lançados no Plano de Ação que devem ser priorizados, se estão sendo priorizados e quais ações foram realmente executadas para o tratamento do item.

Nesse relatório o Encarregado de Proteção de Dados pode analisar, por exemplo, como mostrado no Resumo, quantos itens estão lançados no Plano de Ação que estão há mais de 30 dias abertos; quantos estão com atividades lançadas para tratamento; com análise de impacto realizada, etc.

Com base nessas informações o Encarregado de Proteção de Dados (ou a equipe multidisciplinar) pode tomar decisões de priorizar determinado item lançado ou verificar porque, de acordo com RUT, NPR, PxI determinado item ainda não foi tratado.

Vale lembrar que se o item está lançado no Plano de Ação é porque existe a demanda para tratamento e esta deve ser resolvida. Além disso, quando for gerado o relatório de impacto para atividade de tratamento, os riscos e ações de adequação relacionados à atividade de tratamento serão apresentados e, caso não tenha nenhum tratamento, poderá evidênciar desatenção ou negligência que poderá acarretar desdobramentos críticos no futuro.

Governança de Plano de Ação com base em RUT e NPR

Código de controle de impressão: 2092954245

Título

#55 Necessário prever a contratação de solução para gestão dos acessos aos sistemas SOX

Tipo de lançamento: Ação de adequação

Data de criação: 14/07/2022

Relação de Probabilidade x Impacto: Media Probabilidade com médio impacto

Nível do risco baseado na relação P x I: 100

Matriz RUT

Relevância: 2, Urgência: 5, Tendência: 5 --- Total: 50

NPR

Severidade: 4, Ocorrência: 10, Detecção: 2 --- Total: 80

Distribuição de tarefas

#1-Tarefa: Contratação de sistema de acesso

Nome do responsável: Norberto Tordin

Data limite para a resposta da tarefa: 25/08/2022

Contém resposta do responsável pela execução? Não

Aceita como executada? Não

Análise de impacto

Impacto: Acessos indevidos

Grau do impacto: 50

Análise do relatório pelos responsáveis

Nenhuma ação de aprovação foi encaminhada para análise!

Encerramento do Plano de Ação

Status do item lançado para tratamento no Plano de Ação: Ainda em aberto.

Resumo

Quantidade total de itens lançados para tratamento no Plano de Ação: 67 - Finalizados: 14

Referentes a RISCOS: 60 - Finalizados: 13

Referentes a AÇÕES DE ADEQUAÇÃO: 3 - Finalizados: 1

Referentes a ITENS DE MONITORAMENTO: 3 - Finalizados: 0

Referentes a VULNERABILIDADES: 1 - Finalizados: 0

Desse total de itens lançados (67), 67 estão há mais de 30 dias abertos.

Desse total de itens lançados (67), 52 não tiveram (até o momento) nenhuma distribuição de tarefa de execução.

Desse total de itens lançados (67), 56 não tiveram (até o momento) nenhuma análise de impacto realizada.

Desse total de itens lançados (67), 64 não tiveram (até o momento) nenhum encaminhamento de análise do item.

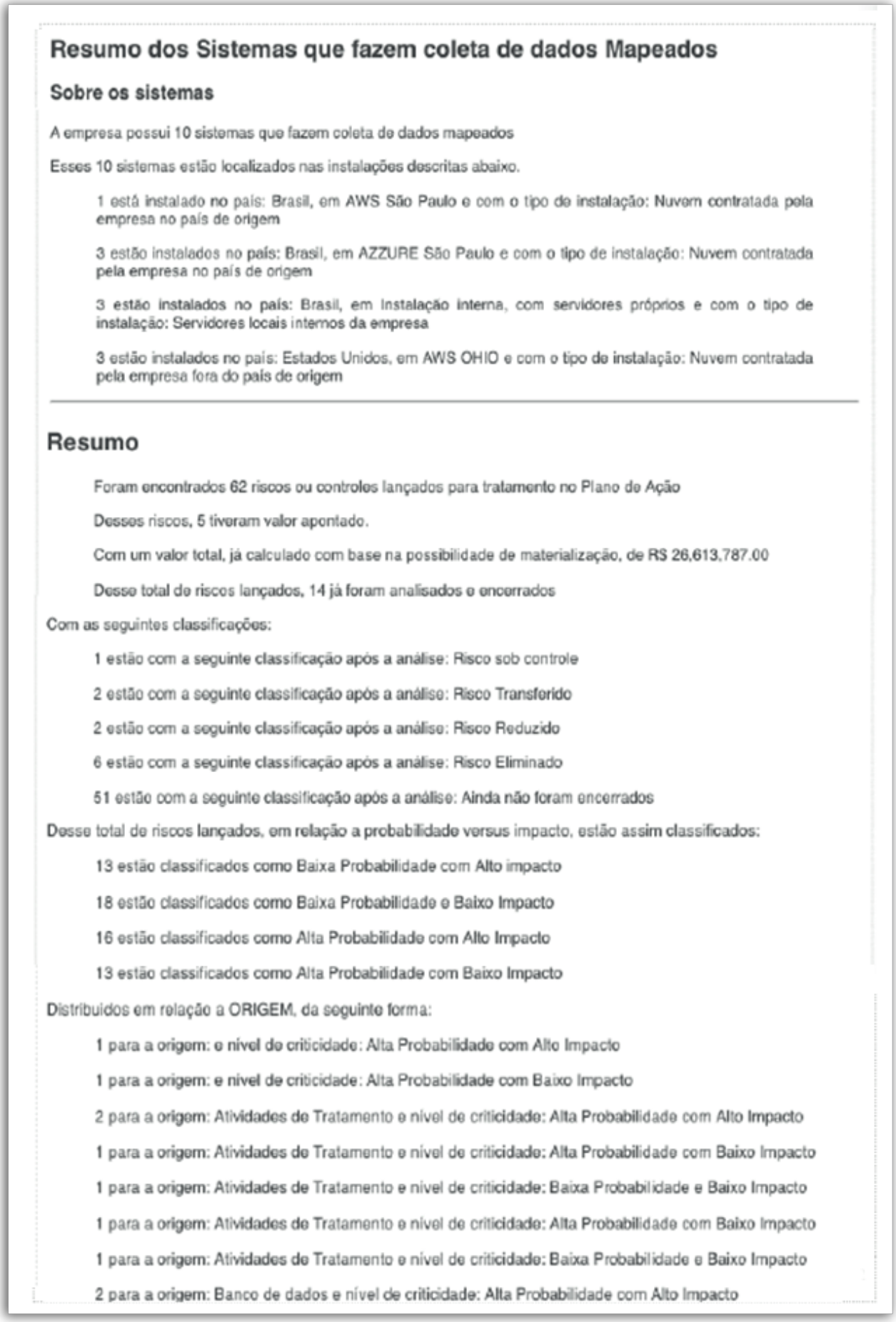
Imagem acima destaca o Relatório de Governança de Plano de Ação com base em RUT, NPD e PxI.

RELATÓRIO
DE IMPACTO BASEADO NOS RISCOS MAPEADOS

Esse relatório tem como objetivo apresentar os riscos e ações de adequação cadastrados durante a fase de mapeamento, assessment e definição das atividades de tratamento.

Com base nessas informações a equipe multidisciplinar poderá analisar o que foi feito no processo de adequação e tomar as medidas de continuidade.

Esse relatório tem o propósito de ser o "entregável" do projeto de adequação, evidenciando os mapeamentos, para cada um dos itens previstos, com os respectivos riscos e ações de adequação que deverão ser executadas.



Resumo dos Sistemas que fazem coleta de dados Mapeados

Sobre os sistemas

A empresa possui 10 sistemas que fazem coleta de dados mapeados

Esses 10 sistemas estão localizados nas instalações descritas abaixo.

1 está instalado no país: Brasil, em AWS São Paulo e com o tipo de instalação: Nuvem contratada pela empresa no país de origem

3 estão instalados no país: Brasil, em AZZURE São Paulo e com o tipo de instalação: Nuvem contratada pela empresa no país de origem

3 estão instalados no país: Brasil, em Instalação interna, com servidores próprios e com o tipo de instalação: Servidores locais internos da empresa

3 estão instalados no país: Estados Unidos, em AWS OHIO e com o tipo de instalação: Nuvem contratada pela empresa fora do país de origem

---

Resumo

Foram encontrados 62 riscos ou controles lançados para tratamento no Plano de Ação

Desses riscos, 5 tiveram valor apontado.

Com um valor total, já calculado com base na possibilidade de materialização, de R$ 26,613,787.00

Desse total de riscos lançados, 14 já foram analisados e encerrados

Com as seguintes classificações:

1 estão com a seguinte classificação após a análise: Risco sob controle

2 estão com a seguinte classificação após a análise: Risco Transferido

2 estão com a seguinte classificação após a análise: Risco Reduzido

6 estão com a seguinte classificação após a análise: Risco Eliminado

51 estão com a seguinte classificação após a análise: Ainda não foram encerrados

Desse total de riscos lançados, em relação a probabilidade versus impacto, estão assim classificados:

13 estão classificados como Baixa Probabilidade com Alto Impacto

18 estão classificados como Baixa Probabilidade e Baixo Impacto

16 estão classificados como Alta Probabilidade com Alto Impacto

13 estão classificados como Alta Probabilidade com Baixo Impacto

Distribuidos em relação a ORIGEM, da seguinte forma:

1 para a origem: e nível de criticidade: Alta Probabilidade com Alto Impacto

1 para a origem: e nível de criticidade: Alta Probabilidade com Baixo Impacto

2 para a origem: Atividades de Tratamento e nível de criticidade: Alta Probabilidade com Alto Impacto

1 para a origem: Atividades de Tratamento e nível de criticidade: Alta Probabilidade com Baixo Impacto

1 para a origem: Atividades de Tratamento e nível de criticidade: Baixa Probabilidade e Baixo Impacto

1 para a origem: Atividades de Tratamento e nível de criticidade: Alta Probabilidade com Baixo Impacto

1 para a origem: Atividades de Tratamento e nível de criticidade: Baixa Probabilidade e Baixo Impacto

2 para a origem: Banco de dados e nível de criticidade: Alta Probabilidade com Alto Impacto

Imagem acima destaca o Relatório Impacto baseado em Riscos Mapeados.

CONCLUSÃO

Tudo o que foi apresentado nesse material tem como principal finalidade a orientação de profissionais, empresas e pessoas dedicadas a projetos e consultorias, tornando possível e mais clara a compreensão das premissas de um projeto de adequação à LGPD, considerando principalmente o "day after", quando a equipe de consultoria entrega o projeto e a empresa precisa dar sequência e manter tudo o que foi definido.

O uso do NCC Data Privacy tanto durante quanto após o projeto, traz vários benefícios, tais como a automação, rapidez, assertividade, segurança e economia, pois sua estrutura de formulários eletrônicos, workflows, bots e integrações, garantem a execução das boas práticas de proteção de dados e privacidade efetivando o compliance com a Lei Geral de Proteção de Dados no dia-a-dia das empresas.

O que destaquei aqui, quanto a Controles e Relatórios, está diretamente ligado a Governança e Compliance, e pode ser entendido também como sendo parte do **"Escritório de Privacidade".**

A NAI-IT é uma empresa de tecnologia da informação com foco em soluções de Governança, Risco, Compliance e Privacidde. Oferecemos ao mercado a Plataforma NCC, NAI Compliance Center, com módulos de Gestão de Identidades e Acessos, Access Control, Data Privacy, Data Discovery e BOT Manager.

nai it

today is your future

SAIBA +

ACESSE:

WWW.NAI-IT.COM.BR

E AGENDE UMA

APRESENTAÇÃO.