E BOOK

# GOVERNANÇA CIBERNÉTICA RN 964/21 ANEEL.

O QUE DEVE SER ATENDIDO.

2023

WWW.NAI-IT.COM.BR

# INTRODUÇÃO

Cibersegurança é um tema que tem ganhado destaque em função de inúmeros ataques a empresas por hackers com pedidos de resgate milionários para que os acessos aos sistemas sejam retomados.

Cibersegurança é a prática de proteger os ativos (computadores, notebooks, servidores,dispositivos móveis) da empresa contra ameaças de acesso para o roubo de informações.

No Brasil ganhou mais notoriedade em função da Lei Geral de Proteção de Dados (LGPD) que tem como princípio base a proteção à privacidade dos dados dos titulares.

O que se busca com a Resolução Normativa 964/21 é justamente uma garantia de que as empresas de geração, transmissão e distribuição de energia do país estejam praticando as
melhores práticas de proteção para que um eventual ataque não prejudique todo o sistema.

O setor de energia foi um dos principais alvos de ataques cibernéticos no Brasil em 2020 e 2021, no auge da pandemia da covid-19, quando as ofensivas dos hackers fizeram vítimas como Copel, EDP, Enel, Energisa, Light, Eletronuclear, entre outras. Neste material o objetivo não é discutir os itens que devem ser atendidos, mas apresentar um breve descritivo para introdução ao tema e, na sequencia, uma descrição de como a NAI-IT pode auxiliar com o projeto com a implantação do NAI Compliance Center.

Aproveite esse conteúdo e sinta-se a vontade em entrar em contato com a NAI-IT para maiores esclarecimentos.

**CIBERSEGURANÇA CONTRA ATAQUES HACKER.**

*“O Setor de Energia foi um dos principais alvos de ataques cibernéticos no Brasil em 2020 e 2021.*

## 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.*

# RESOLUÇÃO DA ANEEL DEFINE REGRAS

## E DIRETRIZES DE SEGURANÇA CIBERNÉTICA AOS AGENTES DO SETOR.

A Resolução Normativa 964, de 14 de dezembro de 2021, da Agência Nacional de EnergiaElétrica (ANEEL), estabelece as regras, diretrizes, políticas e o conteúdo mínimo que os agentes do setor de energia elétrica devem seguir no contexto da segurança cibernética no relacionamento com o Operador Nacional do Sistema Elétrico.

O ONS estabeleceu prazos para que os agentes pudessem se adequar às medidas de segurança cibernética constantes no Manual de Procedimento da Operação- Módulo 5, Sub módulo 5.13. Esses prazos foram definidos com base na data da publicação do regulamento, em 09 de julho de 2021.

O primeiro grupo de medidas teve o prazo expirado em 09 de janeiro de 2023 e, portanto, já sujeitos a fiscalização por parte do ONS.
Essas medidas buscam garantir a segurança cibernética aos dados das empresas e evitar que acessos indevidos sejam propagados para as demais empresas ou ONS.

## O QUE DEVE SER ATENDIDO?

Foram estabelecidos nesta resolução e manual de procedimento de operações os tópicos que devem ser previstos para atendimento das empresas para a adequação ao disposto na referida Resolução Normativa:

4.1- Arquitetura tecnológica para o ambiente.
4.2-Governança de segurança da informação.
4.3- Inventário de ativos.
4.4- Gestão de vulnerabilidades
4.5- Gestão de acessos
4.6- Monitoramento e Resposta a incidentes

Base: Manual de Procedimento da Operação – Módulo 5, Sub módulo 5.13. Publicado em 09/07/2021.
https://www.ons.org.br/AcervoDigitalDocumentosEPublicacoes/RO-CB.BR.01_Rev.00.pdf

# 4.1 - ARQUITETURA TECNOLÓGICA PARA O AMBIENTE.

Esse item do Manual de Procedimentos da Operação prevê que a empresa implemente alguns itens operacionais, como a segregação em zonas de segurança.

No item 4.1.3, no entanto, há menção para que o acesso externo (redes externas da organização) somente pode ser permitido para o desempenho de atividades autorizadas. E esse acesso somente deve ser realizado por meio de Rede Privada Virtual (VPN).

Como característica desse item 4.1.3 nota-se que deve existir medidas técnicas e administrativas para garantir que o acesso a VPN somente seja concedido para as pessoas (funcionários, terceiros, etc) que efetivamente tiverem necessidade desse tipo de acesso, ou seja, o item 4.5 está intimamente relacionado com o disposto neste item 4.1.

**O QUE DEVE SER ATENDIDO.**

# 4.2 - GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO.

Esse item do Manual de Procedimentos da Operação é mais simples na sua definição e prevê que a empresa deve nomear os gestores e responsáveis pela Governança.

No item 4.2.2, diz que deve ser estabelecida política (que no nosso entender poderia ser definido no plural para ficar mais compreensível) para definir os papéis e responsabilidades em relação à segurança cibernética.
Algo que pode parecer realmente simples, em nomear quem serão os gestores e responsáveis, mas pode ficar mais complexo de acordo com a exigência na definição das políticas de segurança da informação. Para nomear os responsáveis é necessário que as políticas de segurança da informação sejam criadas, aprovadas e divulgadas.

# 4.3 - INVENTÁRIO DE ATIVOS.

Esse item do Manual de Procedimentos da Operação prevê que todos os ativos, softwares, hardwares sejam **inventariados**, minimamente a cada 24 meses.

No item 4.3.2, diz que o **inventário dos ativos** deve ser **armazenado de forma segura**, com políticas de armazenamento bem definidas, com **acesso restrito** às pessoas que necessitem das informações para o **exercício de suas funções**.

Quem será responsável por fazer esse inventário, armazena-lo de forma segura e ainda garantir o acesso restrito das informações a quem de direito?

Será que 24 meses para manter o inventário é um prazo razoável, se levarmos em consideração o quanto de novas tecnologias e formas de acessos indevidos são publicadas e verificadas pelos softwares de análise de vulnerabilidades a cada dia?

Imagine uma rede com 1.000 ativos para serem inventariados manualmente, o quanto de esforço e pessoas seria necessário.

# 4.4 - GESTÃO DE VULNERABILIDADES.

Esse item do Manual de Procedimentos da Operação prevê que os pacotes de correção dos softwares, hardwares, sejam implementados para todas as tecnologias conectadas ao ARCiber.

No item 4.4.1, alínea b, diz que deve ser feito o mapeamento dos ativos inventariados para as atualizações disponibilizadas pelos fabricantes.

Com base no que foi citado no item 4.3 (Gestão de ativos), a respeito de quem vai fazer esse inventário, adicione um item a mais na atividade que é acompanhar as vulnerabilidades encontradas nos ativos que forem relacionadas a atualizações (embora num contexto de vulnerabilidade esse seja apenas um dos itens a verificar) de cada software ou hardware. E manter isso atualizado.

Caso um novo software tenha sido instalado em determinado computador e ainda não passou pelo inventário. Será que existe alguma vulnerabilidade a ser verificada?

# 4.4 - GESTÃO DE ACESSOS.

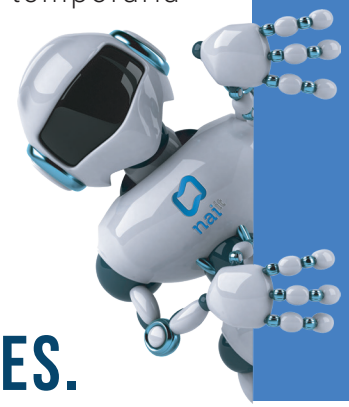
Esse item do Manual de Procedimentos da Operação prevê que deva **existir política de gestão de identidades e acessos.**

Todos os artigos desse tópico, que é bem extenso por sinal, fazem referência a implementação, com **governança**, para a **gestão de identidades e acessos** inclusive com **políticas de segurança da informação** para a gestão das senhas.

No item 4.5.1.1 cita que as credenciais de acesso devem ser individuais e aprovadas pela alçada competente.

O conceito de gestão de identidades e acessos deve ser previsto na sua plenitude, pois ao pensar em conceder o acesso, mesmo que seja com critérios de aprovação, deve-se pensar nas revogações, seja de forma temporária ou definitiva.

Sugiro a leitura do nosso e-book específico sobre Gestão de Identidades e Acessos como complemento a esse conteúdo.



O QUE DEVE SER ATENDIDO

# 4.6 - MONITORAMENTO E RESPOSTA A INCIDENTES.

Esse item do Manual de Procedimentos da Operação prevê que os ativos devem estar configurados para gerar logs de segurança apropriados.

Todos os artigos desse tópico fazem referência a implementação de controles que validem
a integridade dos ativos e que seja estabelecido um plano de resposta a incidentes para tratar cada um desses possíveis incidentes.

Como executar o monitoramento e garantir que os ativos estão protegidos e que nenhum incidente de segurança possa permitir que dados sejam acessados indevidamente?

Sugiro a leitura do nosso e-book específico sobre Privacidade, com os controles e relatórios de governança que apresentam as evidências do que está sendo feito na empresa para esses controles.

nai it

today is your future

# GOVERNANÇA, RISCO E COMPLIANCE

A NAI-IT é uma empresa de tecnologia da informação que tem como foco atender demandas de software para Governança, Risco, Compliance e Privacidade.

Temos mais de 15 anos de experiência no segmento de GRC, com clientes de grande porte como Raizen, Shopping Iguatemi, Sonda IT, ZOOP, dentre outros.

Nossa metodologia de implantação tem como premissa atender as demandas do cliente, com resultados que possam ser verificados muito rapidamente.

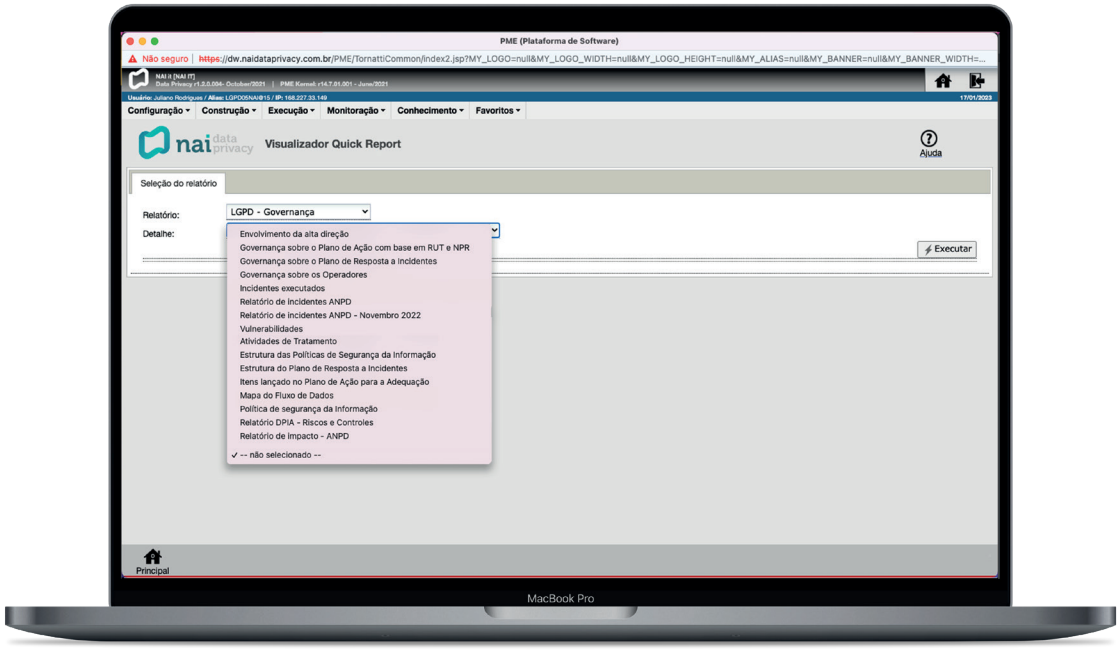
Conseguir identificar e definir o nível de maturidade para evoluir gradativamente com os recursos que o Compliance Center oferece é um trabalho conjunto entre nossos especialistas e a equipe do cliente.

Em alguns clientes onde a dificuldade interna de definir um especialista no tema para ser o elo de ligação entre o cliente e a NAI-IT, nós podemos designar esse especialista do nosso time, exclusivamente para o cliente, para que todas as demandas dos projetos possam ser conduzidas com o mínimo esforço por parte do cliente.

## COMPLIANCE CENTER

- GESTÃO DE IDENTIDADES E ACESSOS (IAM)
- ACCESS CONTROL E MATRIZ SOD
- GESTÃO DA PRIVACIDADE (LGPD/GDPR/ADPPA)
- GESTÃO DE ANÁLISE E GOVERNANÇA (DATA DISCOVERY)
- GESTÃO DE COOKIES (LGPD/GDPR)
- AUTOMATIZAÇÃO DE PROCESSOS DE NEGÓCIO

**O Nai Compliance Center é a plataforma completa que atende a todas as demandas para Governança, Risco, Compliance e Privacidade.**




# NAI COMPLIANCE CENTER

## ATENDIMENTO DE TODOS OS REQUISITOS LISTADOS NO MANUAL DE PROCEDIMENTO DA OPERAÇÃO INSTITUÍDO PELO ONS.

Com o módulo de Gestão de Identidades e Acessos você terá a automação completa dos acessos aos sistemas, com conectores que ficam lendo os eventos gerados pelo RH para identificar quais desses eventos lançados devem ter ação em algum dos sistemas controlados.

Pode ser novos funcionários, promoções, mudanças de unidade de negócios, afastamentos por doença, afastamentos por maternidade, férias, demissões. Tudo o que for lido será avaliado pelas regras de negócio para identificar, de maneira totalmente automática, o impacto nos sistemas destino e aplicar o que deve ser aplicado conforme o evento verificado.

E, para garantir a Governança, todos os eventos são auditados, individualmente para cada funcionário e para cada sistema que teve o evento tratado.

Dessa maneira, se for necessário, a qualquer tempo, identificar quais os acessos que um determinado funcionário tem nos sistemas, basta acessar a ficha do usuário. E ainda mais, se for necessário conhecer qual a regra de negócio que permitiu determinado acesso, isso também será possível. Auditoria e rastreabilidade total.

Assim, o que está descrito no artigo 4.1.3, referente a permitir o acesso à VPN somente a quem de direito, basta ter uma regra cadastrada definindo quem deve ter esse direito que o acesso será concedido e controlado para, caso o funcionário seja demitido, esse acesso seja imediatamente revogado.

No item 4.5, referente a Gestão de Acessos nem precisa se estender muito pois tudo o que está descrito no procedimento será plenamente atendido e com alguns recursos complementares que nem sequer constam na listagem do que deve ser atendido.

Podemos destacar ainda como principais recursos, pensando no disposto do referido regulamento, mas também no uso de forma efetiva para todos os sistemas da empresa:
**Matriz de Risco Cruzada e Segregação de Função**: Esse recurso permite que seja criado uma matriz de risco envolvendo todos os sistemas da empresa, de forma que seja possível cadastrar conflito de perfil de um sistema com um perfil de um outro sistema diferente. Por exemplo, caso a empresa tenha um sistema de pedidos de compra e um outro sistema financeiro, e seja necessário controlar para que no sistema "A" com perfil de compra, um usuário não tenha o perfil de pagamento no sistema "B", isso seja validado antes da concessão e, dependendo do modelo implementado, disparado via workflow para aprovação dos gestores e de quem for necessário.

Muitas vezes as pessoas se esquecem dos acessos concedidos em sistema operacional. Quando for Windows, tem o Active Directory que deve ser utilizado como base de controle. Mas quando for Linux, alguns usuários, dependendo do perfil de acesso podem ter também acesso criado no próprio sistema operacional. Em caso de demissão, onde os acessos precisarão ser revogados, será que esse acesso ao Linux será lembrado? E, se esquecido, pode dar muito poder para o usuário caso consiga o acesso.

Com o Compliance Center esse problema também não existirá, pois esse acesso também será revogado automaticamente.

**Ratificação dos acessos:** Ratificar acessos é uma das grandes dores na maioria das empresas. Ratificar acessos é passar para o Gestor a tarefa de analisar para cada funcionário quais são os acessos que estão atribuídos com a finalidade de validar se esse determinado funcionário deve ter mesmo os acessos que foram concedidos. E isso é feito manualmente em várias empresas, com o encaminhamento por e-mail ao gestor a relação dos funcionários e respectivos acessos para validação. Além de trabalhoso ao extremo para gerar as planilhas, tem um outro trabalho imenso que é ler o que foi marcado como não devido e aplicar em cada um dos sistemas. E isso é uma tarefa a mais que acumula para o pessoal de TI.

Com o uso do Compliance Center essas tarefas são todas automatizadas e podem ser inclusive, programadas com intervalos de data para serem executadas. Assim, quando for necessário uma ação de ratificação de acessos, os robôs do Compliance Center identificarão a necessidade, montarão a estrutura e dispararão um workflow para o Gestor, com um formulário eletrônico para que o gestor marque, apenas, quais perfis devem fazer parte da lista do respectivo funcionário.

E quando terminar a análise, os robôs interpretarão o retorno e farão o encaminhamento para o IDM aplicar em cada um dos sistemas, a revogação dos perfis que foram marcados pelo gestor. Isso, com zero interferência humana e executado assim que o gestor finalizar a análise.

Mas cabe ainda uma ressalva nesse quesito da Ratificação dos Acessos.

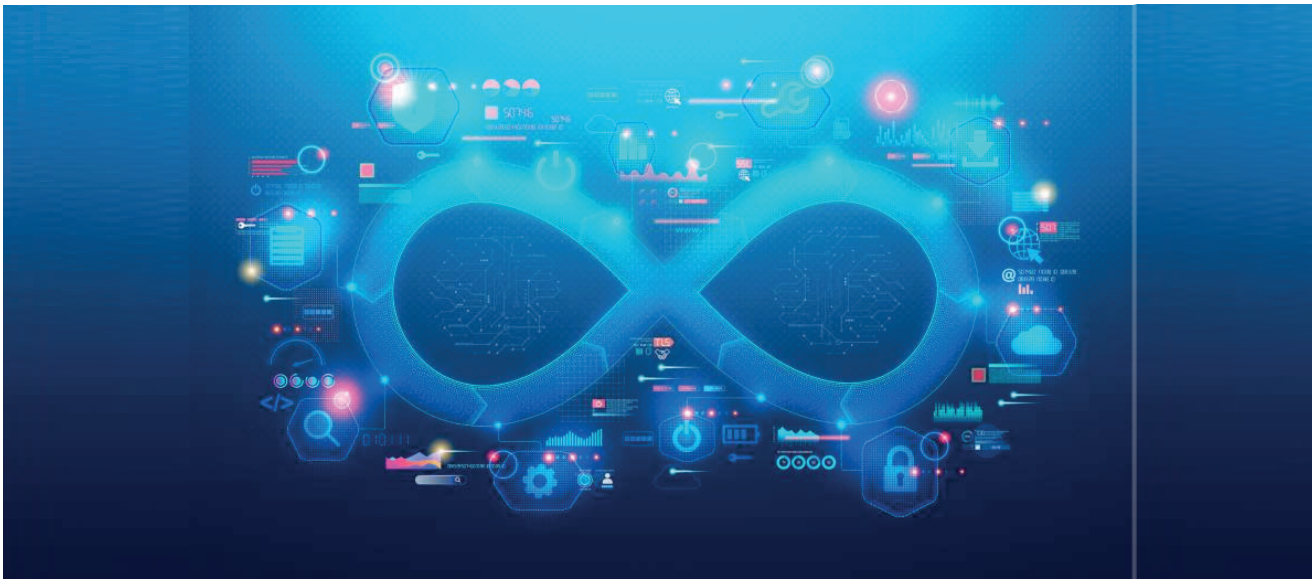
Executar a Ratificação pode ser uma exigência de auditoria e portanto deve ser cumprida e com todas as evidências necessárias registradas. Mas como todo o processo de concessão, a revogação dos acessos é automatizado por regras e existem robôs para executarem as integrações nos sistemas. Portanto, muito provavelmente não haverá acesso indevido concedido a nenhum funcionário.

E supondo que caso um acesso específico tenha que ser concedido, mesmo que "quebrando" a regra da matriz de risco, mas com a devida aprovação da equipe de Governança, esse acesso pode ser concedido com prazo de validade. Quando atingir a data limite, automaticamente esse acesso será revogado, mantendo a estrutura de acesso totalmente integra e saneada.

A qualquer momento que seja necessário comprovar ou apresentar relatórios para a auditoria (interna ou externa) ninguém vai precisar se preocupar e validar anteriormente ou passar horas ou dias atendendo a equipe de auditoria.

**Last Logon**: Atende aos requisitos do Marco Civil quanto a regras que definem quando um determinado usuário executou seu último acesso. Esse procedimento do Compliance Center faz as validações e conforme as regras definidas, faz a revogação automática dos acessos não executados no último intervalo de 365 dias.

**Contas Administrativas:** Esse recurso permite que acessos que sejam considerados críticos e com níveis de acesso mais amplo sejam controlados pelas Contas Administrativas. E essas contas administrativas ficam ligadas a uma conta de usuário. Esse recurso permite um controle muito mais amplo dos acessos e em caso de demissão do funcionário que detinha o direito de uso da conta administrativa, o Compliance Center identifica essa "deficiência" e abre automaticamente um workflow para o gestor indicar quem será o substituto a assumir a conta administrativa.



# GESTÃO DA PRIVACIDADE E CIBERSEGURANÇA

Complementando o que deve ser atendido como requisito no Manual de Procedimento e Operação, vários tópicos listados fazem referência a privacidade e cibersegurança. De uma maneira geral o Manual faz total menção a cibersegurança, mas vamos entender como o Compliance Center atende ao disposto na Resolução Normativa 964.

No item 4.2.2 tem a referência a Política de Segurança. Cabe a empresa definir e implementar a governança para a política de segurança da informação. Nesse item diz sobre definir os papéis e responsabilidades, mas fazer isso sem ter uma política definida, como atribuir responsabilidade?
Com o Compliance Center a empresa poderá cadastrar quem são esses responsáveis pela Segurança da Informação e pode também cadastrar as políticas. E para prever o conceito da governança, as políticas devem ser criadas com o período para revisão e quem são os gestores ou diretores que devem aprovar a política.

Além disso, ao definir a política é possível informar quais são os procedimentos de controle para cada tópico da política que deve ser utilizado para monitoramento e geração de evidência. Nas datas marcadas para o monitoramento os robôs do Compliance Center abrirão automaticamente um novo item no Plano de Ação para que o responsável execute os processos indicados no controle de monitoramento. Se houver necessidade de envolvimento da alta direção, esse responsável poderá indicar quem deve ser acionado que o workflow do sistema fará o disparo e controle de retorno do que foi pedido.

No item 4.3, Inventário de Ativos e 4.4, Gestão de Vulnerabilidades, os procedimentos também são automatizados. Integrado ao Compliance Center temos um software que faz a análise de vulnerabilidades e inventário de ativos.

Essa integração permite que ao identificar um novo ativo na rede, automaticamente esse ativo seja criado na estrutura e, mais do que isso, caso tenha alguma vulnerabilidade ou risco nesse ativo, a integração criará os lançamentos de controle no ativo para que sejam devidamente tratados pelos responsáveis.

Ao identificar uma vulnerabilidade de um ativo, caso essa vulnerabilidade tenha um código CVE cadastrado e esteja com o Plano de Resposta a Incidentes atualizado, se esse CVE demandar a abertura de um tratamento de incidente, isso será feito imediatamente e todas as ações previstas serão executadas conforme o mapeamento.

Toda identificação citada na Resolução será identificada e armazenada na estrutura. Cada endereço IP lido estará relacionado a um determinado ativo. Para cada ativo, quais são os softwares que estão instalados e para cada software instalado, quais os riscos e vulnerabilidades. Se for um risco, deverá ser tratado pelo Plano de Ação. Se for uma vulnerabilidade crítica, deverá ser tratado pelo Plano de Resposta a Incidentes.

No item 4.6, Monitoramento e Resposta a Incidentes, já citamos alguns recursos, mas o Compliance Center ainda oferece muito mais recursos que podem ser utilizados.

Primeiro que pode ser catalogado cada tipo de incidente e para cada tipo de incidente todos os parâmetros de tratamento.

É evidente que cada incidente pode demandar ações e controles diferentes. Por esse motivo que o Compliance Center permite essa categorização individualizada.

Por exemplo: Roubo ou perda de notebook com Acesso indevido por hacker.

Ambos são incidentes de segurança que devem ser tratados, mas tanto em prioridade como criticidade as ações a serem tomadas são específicas.

Ao montar o Plano de Resposta a Incidentes é possível parametrizar quais são as ações que devem ser executadas quando um incidente de segurança for materializado. Quais as ações que devem ser executadas quando for possível identificar uma possibilidade de materialização de um incidente e quais as ações que devem ser executadas como medidas preventivas para o incidente.

Tudo isso controlado pelo workflow do Compliance Center. E no caso das ações preventivas, de acordo com a periodicidade cadastrada os robôs identificam e disparam as ações conforme o mapeamento de datas.

Isso tudo vai gerando **evidências e governança**. Pense na possibilidade de ter uma ação a ser executada que tenha que ter a ciência ou envolvimento da alta direção. Isso é um fato importante a ser observado em critérios de governança, pois dependendo do que for necessário, somente a alta direção pode definir o procedimento a seguir. Dá para fazer manualmente e por e-mail? Dá, mas como fica as evidências e a governança?

Ainda no contexto do Plano de Resposta a Incidentes, temos as definições da LGPD para os incidentes que envolverem acesso a dados pessoais sensíveis. Pela lei a empresa tem prazos definidos para entrega e protocolo do Comunicado de Incidente de Segurança e Comunicado aos Titulares de dados afetados. Isso tudo pode ser feito usando o Compliance Center.

E, não menos importante, em caso de um incidente de segurança, pode ser mapeado o Plano de Continuidade de Negócios. Ao disparar as ações do Plano de Resposta, o que estiver definido no PCN também será automaticamente disparado.

# ATAQUES
## CIBERNÉTICOS

Estudo realizado pela ANPPD em 2021 demonstra que o Brasil foi alvo de 88,5 bilhões de tentativas de ataques cibernéticos. Isso representa um aumento de 950% em relação a 2020.

Somos o segundo lugar no ranking da América Latina. Recentemente o anúncio de ataques cibernéticos só tem aumentado e a proporção de dados atingidos crescendo dia a dia. Em maio de 2022 um ataque cibernético no setor bancário expos dados de contratos de aproximadamente 53 mil clientes.

**88,5 BILHÕES DE ATAQUES EM 2021, UM CRESCIMENTO DE 950% EM RELAÇÃO A 2020.**

# PRÓXIMOS PASSOS

Para atender às disposições da Resolução Normativa ANEEL 964/2021, terão que ser implementados os seguintes requisitos.

De acordo com o planejamento apresentado devemos prever após a implantação do Compliance Center:

**1** - Criar as políticas de segurança da informação com seus respectivos responsáveis e controles.

**2** - Criar o Plano de Resposta a Incidentes e o Plano de Continuidade de Negócios.

**3** - Parametrizar o software de análise das vulnerabilidades para gerar os dados de análise e inventário dos ativos.

**4** - Mapear a arquitetura de conectores e sistemas para a Gestão de Identidades e Acessos.

**5** - Implementar os conectores de leitura e integração com os sistemas controlados.

**6** - Mapear e planejar a evolução do projeto.

# CONCLUSÃO

Existe uma demanda originada pelo ONS, que não é opcional e que deve ser atendida no que diz respeito aos procedimentos de cibersegurança.

O prazo para a primeira fase expirou em 09/01/23, portanto já sujeitando as empresas às sanções que o ONS poderá impor.

Pensar em atender aos requisitos sem o apoio de uma estrutura tecnológica de software será uma ilusão e não terá como ser sustentada.

A NAI-IT é uma empresa que tem a tecnologia necessária, com possibilidade de atender a todos os requisitos listados na Resolução Normativa e no Manual de Procedimento da Operação, de uma forma que permite além de atender ao requisito, trazer benefícios e ganhos operacionais que podem resultar, inclusive, com processos mais estruturados e com redução de custos nos departamentos envolvidos.

nai it

today is your future

**AGENDE UMA APRESENTAÇÃO.**

**NÃO ESPERE TER O PROBLEMA PARA DEPOIS VER COMO RESOLVER!**

**HTTPS://COMPLIANCECENTER.NAI-IT.COM.BR**