DESENVOLVE

DESENVOLVE - AGENCIA DE FOMENTO DE ALAGOAS

Rua Dep. José Lages, 972 - Ponta Verde, Maceió - AL, CEP: 57035-330

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão 3

Maceió - Alagoas

2023

Rev.	Revisão	Data da Revisão	Diretor Presidente	Data da Aprovação
03	(Eduardo Silva, Rogerio Portela, Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

DESENVOLVE

DESENVOLVE - AGENCIA DE FOMENTO DE ALAGOAS

Rua Dep. José Lages, 972 - Ponta Verde, Maceió - AL, CEP: 57035-330

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Política de Segurança Cibernética da Desenvolve - Agencia de Fomento de Alagoas, para Política da Segurança e incidentes com objetivo de proteger a empresa contra possíveis ataques cibernéticos e as ações desenvolvidas em conformidade com a Resolução 4893 do Banco Central do Brasil.

Maceió- Alagoas

2023

Rev.	Revisão	Data da Revisão	Diretor Presidente	Data da Aprovação
03	(Eduardo Silva, Rogerio Portela, Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

DESENVOLVE

SUMÁRIO

1 IDENTIFICAÇÃO....4

2 OBJETIVO....5

3 DIRETRIZES GERAIS....5

4 DIRETRIZES ESPECÍFICAS....8

5 SEGURANÇA LÓGICA DE COMPUTADORES, REDES E SISTEMAS APLICATIVOS....12

6 DEFINIÇÕES....18

7 INDICADORES DE DESEMPENHO....19

8 RESPONSABILIDADES....20

9 PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO....23

10 PLANO DE RESPOSTAS A INCIDENTES....33

11 ANÁLISE E GERENCIAMENTO DOS RISCOS....46

12 ROTINAS DOS SISTEMAS:....53

13 SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENDO DE DADOS EM NUVENS....54

14 FIREWALL....54

15 COMUNICAÇÃO....56

16 ANEXO: POLITICAS OPERACIONAIS E PROCEDIMENTOS OPERACIOANAIS....56

17 ANEXO....57

18 ARTEFATOS RELACIONADOS....68

1. IDENTIFICAÇÃO:

Título:	POLÍTICA DE SEGURANÇA CIBERNÉTICA											
Restrições para Uso:	Acesso						Controle					
	X	Livre		Reservado		Confidencial	X	Controlada		Não Controlada		Em Revisão

1 - RESPONSÁVEIS

Etapa	Área Responsável	Cargo	Data
Elaboração	Superintendência de TI	Superintendente de TI	01/03/2023
Verificação	Governança	Risco	01/03/2023
		Compliance	
Aprovação	Diretoria Executiva	Diretor Presidente	01/03/2023
Distribuição	Compliance	Governança	01/03/2023

2 – DOCUMENTOS DE REFERÊNCIA

Documento	Data	Objetivo
Resolução 4.658	26-04-2018	Dispor sobre a Política de Segurança Cibernética
Súmula Bacen 02697	12-11-2020	Registrar a obrigatoriedade da criação da Política de Segurança Cibernética
Politica de Segurança	19-11-2019	Política de Segurança da informação
Procedimento TI	15-10-2019	Procedimento das Rotinas de Segurança do Setor de TI

3 – REVISÕES

Número		Data	Histórico do Resumo	FOLHA
01		02/12/2020	Emissão inicial	Todas
Revisões	02	22/02/2022	Revisão	Todas
	03	05/06/2023	Revisão para adequação a Resolução 4893	Todas

Rev.	Revisão	Data da Revisão	Diretor Presidente	Data da Aprovação
03	(Eduardo Silva, Rogerio Portela, Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

2. OBJETIVO:

A Politica de Segurança Cibernética da Desenvolve/AL, estabelece diretrizes, regras, e controles em todos os niveis da empresa, incluindo o gerenciamento dos riscos de segurança da informação e segurança cibernética. Seu escopo abrange o direcionamento estratégico para assegurar a proteção efetiva das informações.

- Manutenção dos riscos de segurança da informação e segurança cibernética em níveis aceitáveis, com a utilização de controles adequados e efetivos, frente aos custos, tecnologia e objetivos de negócio;
- Proteção adequada das informações e dos ativos de informação da Desenvolve/AL contra acessos indevidos ou não autorizados;
- Disseminação da cultura de segurança da informação e segurança cibernética;
- Apoio da alta administração na gestão efetiva de segurança da informação e segurança cibernética;
- Destinação das informações somente às finalidades devidamente aprovadas pela Diretoria da empresa;
- Consonância com os princípios estabelecidos no Código de Conduta da Desenvolve/AL;
- Conformidade com normas internas e externas, leis e regulamentações vigentes;
- Observância das diretrizes, objetivos e controles de segurança da informação e segurança cibernética da empresa por parte dos colaboradores e usuários.

Todos os usuários que compõem as estruturas organizacionais da entidade (di-rigentes, colaboradores e estagiários) e demais pessoas com acesso autorizado às informações da Desenvolve/AL, incluindo clientes, parceiros, empresas prestadoras de serviço e ao público em geral.

3. DIRETRIZES GERAIS:

A. TRATAMENTO DA INFORMAÇÃO

A informação sob custódia da instituição mesmo que pertencente a clientes, colaboradores ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

O acesso, geração, utilização, classificação, modificação, distribuição, transferência, armazenamento e eliminação da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados.

A instituição reservar-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada, pelo tempo determinado pela instituição, legislação ou regulação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

B. ACESSO À INFORMAÇÃO

O uso de redes externas de comunicação (Internet, redes privadas etc.) deve ser controlado através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivirus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser

controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo–se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada e após aprovação, utilizaremos via VPN.

Adicionalmente, quando o acesso externo for realizado com o propósito de Home Office, deve ser observada e seguida a Política de Home Office disponível em nossa Intranet.

A remessa de dados da organização, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

C. SISTEMAS APLICATIVOS

Sistemas aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Sistemas aplicativos desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de

atividades críticas do sistema. Onde for impraticável implantar a segregação, outros controles como monitoração das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos sistemas os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso. Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga (Capacity Planning).

4. DIRETRIZES ESPECÍFICAS:

A. TRATAMENTO DA INFORMAÇÃO

Para o conjunto de informações utilizado por um sistema aplicativo, o Comitê Diretivo de Segurança e Contingência deve designar dois proprietários, diretores da instituição, sendo um deles representante da área operacional (Diretor Administratrivo e Financeiro) e o outro da área de negócios a ser indicado pela Diretoria responsável.

São atribuições dos proprietários das informações:

Nomear o gestor das informações, a quem cabe propor as regras de acesso às referidas informações, e administrá-las operacionalmente; e

Aprovar as regras de acesso às informações, conforme proposta do gestor.

Cada gestor de informações indicará um gestor substituto, a ser aprovado pelos proprietários, que deverá exercer suas funções em caso de ausência.

Cada gestor da informação e seu substituto receberão um login diferenciado para exercer esta função, ou seja, configurar os sistemas para atender às normas abaixo descritas para tratamento da informação, bem como a concessão de acessos a usuários.

B. Normas para tratamento da informação

Devem ser definidas regras claras para proteção da informação contra perda, alteração, acesso por pessoas não autorizadas, trilha e logs de atividade e rastreabilidade, seja qual for o meio em que vier a ser armazenada (eletrônico, magnético, impresso etc.).

Devem ser claramente definidos os usuários (empresas, áreas, pessoas etc.) das informações, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não-autorizadas, independentemente da forma como estiver disponível. Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da empresa. Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda.

Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização. É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade das Instituições, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Diretoria responsável, e das quais os colaboradores venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

Os usuários devem adotar a prática de classificação da informação com o objetivo de fornecer o tratamento adequado à informação no aspecto de sua confidencialidade. A orientação sobre a classificação da informação está disponivel na Política interna de Classificação da Informação.

C. Recomendações para o tratamento da informação

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco.

As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa.

Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do colaborador que necessita do suporte. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento, conforme Política Interna de Descarte de Meios Magnéticos de Armazenamento de Informação.

Os gestores devem determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:

D. Riscos inerentes às informações:

- Acesso por pessoas não autorizadas;
- Alteração, utilização, classificação, modificação, distribuição, transferência armazenamento ou eliminação indevida; e
- Indisponibilidade.

E. Consequências:

- **Fraudes:** Possibilidades de lesarem empresas do Conglomerado ou terceiros (clientes, fornecedores etc.);
- **Problemas legais**: Possibilidades de gerar prejuízos, multas, penalidades ou embaraços às Instituições, Diretores e Colaboradores da instituição, a outras pessoas físicas ou jurídicas;
- **Perda de negócio**: Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;

- **Prejuízo de imagem da instituição**: Possibilidades de prejudicar a imagem da Instituição ou de seus colaboradores;
- **Problemas de recuperação**: Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

F. Segurança quanto às pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos da Instituição.

G. Identificação das pessoas

Todas as pessoas com acesso aos sistemas e informações, pertencentes a Instituição, deverão ter uma única identificação (login). As exceções deverão ser devidamente documentadas e aprovadas pelo Comitê Diretivo de Segurança e Contingência.

H. Declaração de Responsabilidade

É um compromisso de responsabilidade direta do colaborador para com as informações, equipamentos e outras propriedades do Conglomerado a ele confiadas,devendo ser lida e assinada quando de sua admissão na instituição.

Este conceito deve ser utilizado também para prestadores de serviço e clientes:

Prestadores de Serviço: a declaração de responsabilidade deve ser uma das cláusulas do contrato.

Clientes: a declaração de responsabilidade deve ser uma das cláusulas do termo de adesão ao produto - ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

A declaração de responsabilidade deve ser lida e assinada, dentro dos formatos aceitos e homologados em meio físico ou eletrônico, por todos os colaboradores antes de ser arquivada na respectiva pasta funcional. O Departamento de Recursos Humanos deve garantir que todos os colaboradores tenham sua declaração deresponsabilidade assinada.

5. SEGURANÇA LÓGICA DE COMPUTADORES, REDES E SISTEMAS APLICATIVOS:

bEste item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse da Instituição.

Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão etc.

Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação.

Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários.

As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

i. Normas para segurança lógica de computadores e redes:

Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada negócio, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles.

Cada gestor da informação é responsável por definir e manter atualizados os

perfis de acesso aos seus aplicativos visando o acesso mínimo necessário para a execução das atividades bem como evitar conflitos de interesse.

ii. Administração do acesso aos sistemas aplicativos:

As informações devem ser analisadas pelos respectivos gestores da informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis ealçadas.

Os sistemas aplicativos devem possuir recursos que possibilitema administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

iii. Administração do acesso de usuários:

Devem existir procedimentos formais que contemplem todas as atividades ligadas á administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários, respeitando as normas vigentees na instituição sobre os acessos aos Sistemas e Diretórios

iv. Controle de acesso a computadores e redes:

Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto.

O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

Os ambientes de produção, homologação e desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

DESENVOLVE

v. Normas para controle de acesso a computadores, redes e sistemas aplicativos:

Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais caracteristicas desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;
- As senhas poderão ser alteradas pelos usuários em qualquer ambiente(operacional ou aplicativo);
- Os sistemas devem ser programados para nunca exibir a senha na tela;
- As senhas devem ser individuais e intransferiveis. A senha é de uso exclusivo,pessoal e intransferível, sendo o compartilhamento proibido em quaisquercircunstâncias;
- As senhas não devem ser triviais e previsiveis;
- Os tipos de caracteres utilizados para a formação da senha devem ser:
- Letras maiúsculas;
- Letras minúsculas;
- Números;
- Sinais ou simbolos especiais (Ex: @ # $ % & * - + = " ' ` ^ ~ { } [ ] / | \ ?!).
- As senhas deverão ter um tamanho mínimo de 08 (oito) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou simbolo especial;
- Os sistemas devem prever um prazo para a expiração de senhas de no máximo (trinta) dias 30.
- Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterá-la no primeiro acesso;
- As senhas trocadas ou expiradas devem ser cadastradas para efeito de

bloqueio de reutilização (mínimo de vinte e quatro senhas);

- Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito;
- Após um máximo de cinco tentativas consecutivas sem sucesso, os acessos devem ser bloqueados até que seja solicitado o desbloqueio do usuário; e
- Uma vez aprovada, a senha deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto, um mesmo usuário não deverá utilizar simultaneamente mais de uma estação de trabalho.

vi. Monitoramento de uso e acesso aos sistemas aplicativos:

Todos os sistemas aplicativos deverão:

- Detectar tentativas de acesso não autorizado;
- Registrar eventos de entrada no sistema (login);
- Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estaçãode rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas; e
- Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

A. Processo de desenvolvimento de sistemas:

Os sistemas desenvolvidos deverão observar e seguir as boas práticas de mercado sobre desenvolvimento seguro a fim de mitigar riscos e vulnerabilidades comumente exploradas nos sistemas. A aderência do processo deve ser realizada através de adequação de processos e/ou uso de tecnologias especificas para esse

tipo de finalidade.

Adicionalmente, cabe à Segurança da Informação avaliar a necessidade de testes de segurança sobre qualquer sistema, seja interno, exposto na internet, hospedado fora da infraestrutura tecnológica da instituição, desenvolvido internamente ou externamente.

B. SEGURANÇA NO ACESSO DE PRESTADORES DE SERVIÇO

Este tópico visa estabelecer controles sobre recursos de processamento da informação da organização durante a execução de serviços por contratados externos.

Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. O que for acordado deve ser explicitado no contrato assinado.

É proibida a utilização de equipamentos próprios do prestador conectados à rede da organização sem a devida autorização escrita pela área de segurança da informação que deverá avaliar a necessidade através de justificativa técnica. Se for necessário deve-se segregá-los em uma rede própria e estabelecer um "firewall" para controlar os acessos.

Caso o prestador utilize softwares próprios em equipamentos da organização, deve-se apresentar documentação ou termo de responsabilidade garantindo direito de uso, que será mantido enquanto o software estiver instalado.

C. Segurança física de computadores

Este tópico destina-se aos usuários e administradores de computadores conectados ou não a uma rede.

O objetivo é garantir que as Instituições estabeleçam, administrem e utilizem computadores de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são

armazenadas e manipuladas através desses equipamentos.

D. Normas para segurança física de computadores:

Os meios de armazenamento considerados como mídias removíveis devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

Os computadores não ligados a uma rede, e que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

***E.* Segurança física dos servidores de rede**

Este item destina-se aos usuários de sistemas operacionais com características de servidores de rede.

O objetivo é garantir que a Instituição administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

F. Normas para segurança física dos servidores de rede:

As mídias removíveis de armazenamento devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

DESENVOLVE

G. Responsabilidades na segurança física dos servidores de rede:

O Anista de infraestrutura , é responsável por:

Elaborar e manter atualizado o inventário de hardware e software; e

Garantir o controle de acesso fisico aos equipamentos.

6. DEFINIÇÕES:

- **Confidencialidade:**
  Garantia de que a informação é acessível somente às pessoas autorizadas;
- **Integridade**:
  Defesa da autenticidade da informação e dos métodos de processamento;
- **Disponibilidade:**
  Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Espaço cibernético**
- **• Incidente de segurança cibernética:**

a) Ameaças internas: ações maliciosas executadas por funcionários, ter ceiros,
contratados e etc.

b) Ataques Destrutivos. Ataques destinados a destruir sua informação ou sistema de informação sem reparo.

c) Extorsão e Ransomware (Vírus).

d) Infecção por Malware.

e) Ataques Web.

f) Ataques DDoS.

- **Ataque cibernético:**

a) Vírus: software que causa danos à máquina, rede, softwares e banco de dados;

b) Cavalo de troia (vírus): aparece dentro de outro software e cria uma

porta para a invasão do computador;

c) Spyware (vírus): software malicioso para coletar e monitorar o uso de informações;

d) Ransomware (vírus): software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- **Risco à segurança cibernética:**

Riscos de ataques Cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis;

- **Ativos tecnológicos: (Físicos e Sistemas):**

Considera-se como **ativo de TI** aqueles itens físicos e virtuais que compõem uma rede corporativa. Portanto, o conceito engloba tanto recursos tangíveis quanto intangíveis.

7. INDICADORES DE DESEMPENHO:

Indicadores	Analisado	Descrição do indicador	Período	Cálculo
Total de Violações	- infecção por vírus ou Malware; - invasão de hackers; - Perda de dados.	Este indicador mede o total de eventos que colocam em risco a segurança dos dados da empresa em um determinado período de tempo.	Semestral	Comparar o total de eventos ocorridos no semestre com o total do semestre anterior.
Tempo médio para Detecção	- O tempo que a empresa leva para detectar um evento de segurança.	Este indicador mostra por quanto tempo as ameaças à segurança estão passando despercebidas na empresa.	Horas	Total de tempo (horas) que o setor de TI leva para identificar as ameaças.

Tempo Médio de Reparo	- O tempo que à empresa leva para corrigir as falhas na segurança.	Se o tempo médio de reparo está aumentando é indício de que talvez seja necessário empregar mais recursos para mitigar as ameaças à segurança dos seus dados, como à implementação de processos ou tecnologias.	Horas	É calculado o momento em que ocorre a falha até o momento em que a correção é realizada e as operações voltam ao normal.
Custo médio por incidente (USTs)	- Custo destinado a cada correção/reparo de incidente ocorrido, (Uma média de 4 a 5 USTs).	Este indicador mostra quanto cada incidente de segurança custa, em média, aos cofres da sua empresa. (Em média R$ 2.000,00 cada UST).	Anual	Somatório do custo de todos os eventos em determinado período e dividir pelo total de eventos analisados.

8.RESPONSABILIDADES:

8.1 Com relação à segurança cibernética, a Desenvolve/AL dispõe das seguintes diretrizes gerais:

8.1.1 Presidência e Conselho de Administração (na sua ausência):

8.1.1.1 Observar e zelar pelo cumprimento da presente Política e quando necessário, acionar os setores responsáveis para consultas sobre as situações que envolvam conflitos da mesma ou mediante a ocorrência de situações nela descritas.

8.1.1.2 Fazer cumprir as diretrizes estabelecidas nesta Política, cobrando a atualização de forma a garantir que quaisquer alterações no direcionamento sejam incorporadas a mesma.

8.1.1.3 Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas

8.1.2 Gestores:

8.1.2.1.1 Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;

8.1.2.2 Realizar a adequada classificação das informações e garantir a continuidade do processamento das mesmas, conforme os critérios e princípios indicados nos normativos internos vigentes sobre o tema;

8.1.2.3 Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;

8.1.2.4 Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a Dados internos e confidenciais, por meio, dentre outros aspectos: (i) da manutenção de softwares antivirus e firewall instalados e atualizados; (ii) da manutenção dos programas de computador instalados no ambiente.

8.1.3 Demais Usuários:

É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias e participe dos programas de conscientização tendo em vistas o cumprimento das diretrizes aqui da Desenvolve/AL:

Possui como objetivo de segurança cibernética: prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético e também:.

8.1.3.1 Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar

acessos, manipulações ou usos não autorizados a dados internos e confidenciais, por meio, dentre outros aspectos: (i) da manutenção de softwares antivirus e firewall instalados e atualizados; (ii) da manutenção dos programas de computador instalados no ambiente;

8.1.3.2 Atender às leis e normas que regulamentam as atividades da Desenvolve/AL;

8.1.3.3 Com relação às medidas de segurança, adota procedimentos e controles para reduzir a vulnerabilidade da Companhia a incidentes e atender aos objetivos de segurança cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

8.1.3.4 Controla, monitora, restringe o acesso aos ativos de informação a menor permissão e privilégios possíveis.

8.1.3.5 Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.

8.1.3.6 Realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da empresa, que abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

8.1.3.7 Identifica os incidentes de segurança de acordo com a classificação das informações envolvidas e o impacto na continuidade dos negócios da Desenvolve/AL.

8.1.3.8 Adota processo de gestão de continuidade de negócios relativo a segurança da informação e cibernética.

8.1.3.9 Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância. Toda informação possui um proprietário e a classificação deste, é obrigatória para assegurar os controles que garantam a confidencialidade.

8.1.3.10 Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico da Desenvolve/AL e que possam ocasionar o comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais.

8.1.3.11 Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

8.1.3.12 A implementação de programa de treinamento para colaboradores;

8.1.3.13 A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos;

8.1.3.14 O comprometimento da alta administração com a melhoria continua dos procedimentos relacionados com a segurança da informação e cibernética.

9.PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO:

Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, a Desenvolve/AL vem adotar procedimentos e controles, conforme porte e perfil de risco da entidade. Estes procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

As informações de propriedade ou sob custódia da Desenvolve/AL, são mantidas em meio eletrônico ou fisico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados;

A partir dessa política, são adotados mecanismos para disseminação da cultura de segurança cibernética na instituição.

Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética no âmbito da Desenvolve/AL, bem como o monitoramento e controle dos riscos à ela relacionados.

Com a presente Política, a Agência de Fomento de Alagoas S.A. assegura o cumprimento da determinação do Bacen, definindo as diretrizes para a realização de testes periódicos de segurança para os sistemas de informações, em especial os mantidos em meio eletrônico.

9.1-Sistemas Informatizados:

O antivírus corporativo, utilizado na Desenvolve, é um sistema de segurança que protege contra os ataques aos arquivos e sistemas corporativos. Dentre os principais recursos, estão:

9.1.1- Segurança: bloqueia ataques direcionados e ataques persistentes avançados com proteção em camadas no endpoint;

- A proteção contra ameaças à rede analisa os fluxos de dados que entram e bloqueia ameaças de forma proativa;
- A análise de reputação da tecnologia Insight™ (anti-vírus) separa os arquivos em risco dos arquivos seguros para permitir uma detecção mais rápida e precisa;
- A análise comportamental da tecnologia SONAR™ monitora o comportamento do aplicativo em tempo real e intercepto ataques direcionados e ameaças de dia zero;
- Proteção de antivírus, antispyware (anti-vírus) e firewall robusta.

9.1.2- Desempenho: Ótimizado para fornecer um desempenho robusto em ambientes físicos e virtuais:

- A tecnologia Insight exige somente a verificação dos arquivos em risco, reduzindo em até 70% o tempo de verificação;
- Tamanho do cliente reduzido com menor espaço na memória para sistemas incorporados;

- Carga de rede reduzida com flexibilidade para controlar o número de conexões e a largura de banda da rede.

9.1.3- Gerenciamento mais inteligente: Console de gerenciamento único em plataformas físicas e virtuais com controle granular de políticas:

- Agente único de alto desempenho com um único console de gerenciamento para Windows, Mac, Linux, máquinas virtuais e sistemas incorporados;
- Suporte para implementação remota e gerenciamento de cliente para Windows e Mac;
- Controle granular de políticas com bloqueio do sistema, controle de dispositivos e aplicativos e detecção de local.

9.1.4- Links de Internet:

A DESENVOLVE-AL tem três links de internet, fibra óptica do ITEC, circuito MPLS da INFOVIA-AL e link GVT, com as seguintes capacidades de 100Mbps, 50Mbps e 50Mbps, respectivamente. Os links estão distribuídos no formato que permite a alta disponibilidade das conexões com a internet.

9.1.5- Firewall:

O Firewall utilizado na Desenvolve, é um equipamento com soluções de segurança integrada (UTM) que protege a rede contra-ataques unificados e ameaças avançadas. É um appliance com proteção integrada e em tempo real que integram as funcionalidades em uma plataforma de altíssima performance, como:

- Unified Threat Management (UTM)
- Antispam
- Antivírus / Antispyware
- Controle de Aplicação
- Data Loss Prevention (DLP)
- Segurança de banco de dados
- Firewall

- Endpoint Protection
- Intrusion Prevention System (IPS)
- IPv6
- VoIP
- Virtual Private Network (VPN) – IPsec e SSL
- Segurança Virtual
- Vulnerabilidade e Gerenciamento de Conformidade
- Otimização de WAN
- Web Filtering
- Web Application Security
- Wireless LAN (WLAN)

O FortiGate Next Generation Firewall utiliza processadores de segurança específicos, serviços de segurança contra ameaças e a inteligência dos laboratórios FortiGuard para fornecer proteção de alto nível e alto desempenho, incluindo tráfego criptografado. O FortiGate reduz a complexidade com visibilidade automatizada de aplicativos, usuários, rede e fornece classificações de segurança para adotar as melhores práticas de segurança recomendadas.

9.1.6- Backup e Restore:

Software de backup e recuperação que fornece proteção abrangente dos dados, análise em tempo real e otimização guiada.

Com base em uma arquitetura unificada que utiliza análise e automação, o protetor de dados da Desenvolve oferece proteção de dados abrangente, inteligência em tempo real e otimização orientada para garantir ações de backup e recuperação simples, confiáveis, inteligentes e econômicas. Ao padronizar o backup e a recuperação das informações espalhadas entre locais, aplicativos, formatos, plataformas de armazenamento, sistemas operacionais e hipervisores, o protetor de dados fornece a segurança para informações de missão crítica do núcleo até a borda

em infraestruturas físicas, virtuais e de nuvem.

Micro Focus Data Protector é uma solução enterprise de proteção de dados que permite o atendimento das condições de segurança de dados, construído de uma forma de otimizar as execuções de backup e restauração de forma diversificada, dinâmica e distribuída nos diversos ambientes da infraestrutura da TI.

Nota 01- Backups e Restore:

- **Diário**: São aqueles Backups novos ou modificados diariamente;
- **Semanais**: São aqueles Backups selecionados e arquivados após 07 dias;
- **Mensais**: São aqueles Backups selecionados e arquivados após 30 dias;
- **Anuais**: São aqueles Backups selecionados e arquivados após 365 dias.

A. Normas para Backup/Restore:

A elaboração do plano de Backup/Restore deverá levar em consideração os aspectos abaixo:

Os períodos de atualização dos dados; e Particularidades de cada Instituição do Conglomerado.

As informações consideradas imprescindíveis devem estar presentes nas rotinas de backups operacional e contingencial, levando-se em consideração a periodicidade deatualização dos dados.

As informações devem estar sujeitas às rotinas de backups operacional e contingencial conforme critério definido pelo usuário.

As cópias de backup devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas.

Deve-se manter uma cópia do plano de Backup/Restore juntamente com o backup contingencial.

Devem ser realizados testes de restore periodicamente, mantendo evidências do último teste realizado.

Devem ser mantidas, no mínimo, as duas últimas versões dos backups operacional e contingencial. Para os backups históricos, a quantidade de versões será determinadapor exigência legal ou norma interna.

B. Plano de Backup/Restore - Conteúdo:

Abrangência: Relação dos arquivos e diretórios a serem copiados no processo de

backup.Periodicidade: Intervalo de tempo após o qual o sistema é submetido à rotina de backup.Retenção: Prazo pelo qual os backups devem ser mantidos.

Procedimentos: Descrição dos procedimentos de backup.

Quantidade de cópias: Número de cópias de backup, locais e meios de armazenamento.

C. Identificação dos meios de armazenamento: Os meios de armazenamento devem estar devidamente identificados.

Registro do uso das cópias de backup: A manipulação dos meios de armazenamentodeve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações.

Manutenção das cópias Backup: Quando o prazo de retenção for superior ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dos dados em novo meio, periodicamente.

D. Responsabilidades quanto ao Backup/Restore

É de responsabilidade do Analista de Infraestrutura, manter e documentar o plano de backups e garantir a execução de seus procedimentos.

E. Testes regulares de armazenamento e recuperação de dados

Todo e qualquer meio de armazenamento assim como os procedimentos de recuperação devem ser regularmente testados, garantindo sua efetividade. A periodicidade deve ao menos ser uma por ano, a ser determinada pelo Comitê de Segurança e Contingência, considerando o nível de risco do negócio. Devem ser mantidas evidências do sucesso dos testes feitos.

F. Pirataria

Este item se destina a todos os usuários e administradores de servidores de redes ou computadores, inclusive portáteis, conectados ou não a uma rede e tem como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de softwares dentro das instalações das empresas do Conglomerado.

G. Utilização Segura de Hardware e Software

Todos os equipamentos portáteis (notebooks, laptops, netbooks, ultrabooks, tablets e smartphones) que tenham capacidade de armazenamento de dados, devem seguir os princípios de segurança contidos nessa política. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, os dados devemser criptografados ou ter seu acesso protegido por senha.

É proibida a utilização de qualquer equipamento particular na rede corporativa doConglomerado Alfa.

É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de "softwares" ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas do Conglomerado ou desenvolvidos por terceiros para o Conglomerado.

H. Acesso à Internet

A Internet abrange vários aspectos e serviços (websites de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades de negócio. A restrição a websites não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede de Internet.

O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (Nome do usuário e endereço acessado são informações obrigatórias no rastreamento).

O usuário deve restringir o acesso aos websites ainda não bloqueados que possam denegrir a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (Webmail, jogos etc.). Deve também comunicar o endereço eletrônico desses websites à área de Segurança da Informação, que deverá realizar seu imediato bloqueio.

O acesso à Internet deve ser feito através de "Servidores de Acesso" protegidos por sistemas de Firewall. Quando for necessário o acesso utilizando uma

segunda conexão através de modem ou rede wi-fi, a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada. Os requisitos de segurança destas máquinas em particular devem serrespeitados (antivírus e firewall local). Casos especificos como esses devem ser aprovados pelos responsáveis da área de Segurança da Informação.

I. Acesso ao correio eletrônico

A instituição disponibiliza aos seus colaboradores a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípiosaplicáveis aos negócios.

J. Plano de continuidade do negócio

Um plano de continuidade do negócio deve garantir a recuperação dos processos críticos do Conglomerado quando da indisponibilidade do ambiente ou de quaisquer recursos que impossibilitem o desenvolvimento ou as operações das áreas de negócio.

É de responsabilidade de cada área envolvida no desenvolvimento dos negócios, elaborar, testar e implantar seus planos de contingência. A área de Tecnologia de Informáção da Desenvolve – AL pode orientar na elaboração desses itens. Adicionalmente, o plano deve ser revisado e atualizado anualmente.

A definição de processos críticos de uma empresa ou área, obrigatoriamente, deve obedecer a critérios emanados pelos Diretores responsáveis pela instituição / área.

K. Pontos a serem observados no plano de continuidade do negócio:

Na elaboração de um plano de continuidade do negócio os pontos abaixo devem serobservados:

- As funções críticas devem ser identificadas e definidas;

- Traçar uma estratégia para recuperação de cada função crítica;
- Priorizar as funções críticas para ordenar sua recuperação;
- Identificar as atividades necessárias para recuperar cada função;
- Quantificar os recursos humanos e técnicos necessários ao cumprimento doplano;
- Documentar os processos críticos;
- Identificar os responsáveis pela recuperação de cada processo ou função;
- Ações para restabelecer a operação normal; e
- Identificar os recursos de backup (infraestrutura, hardware, software, sistemas aplicativos e telecomunicações).

L. Revisões periódicas do plano de continuidade do negócio:

- O plano de continuidade do negócio deverá sofrer revisões anuais a fim de identificarpontos que estiverem em desacordo com a situação atual. Deverão ser observados os pontos abaixo:
- Troca de fornecedores ou contratados;
- Alteração de endereços ou números de telefones;
- Mudanças nas prioridades de recuperação;
- Interdependência entre sistemas e aplicativos;
- Mudanças nas funções e nos processos críticos de negócio;
- Mudanças nas práticas operacionais; e
- Atualização da relação de colaboradores críticos.

M. Canais de relacionamento com o cliente

- Os seguintes canais eletrônicos de relacionamento devem garantir a positivação de informações do cliente:

- Offline: através de número da conta e senha de acesso ou de confirmação de informações de conhecimento pessoal do cliente.
- Internet Banking e Aplicativo Móvel: através de CPF, senha de acesso e chave se segurança ou confirmação de informações de conhecimento pessoal do cliente.
- SAC: através de CPF e confirmação de informações de conhecimento pessoal docliente.
- WhatsApp (corporativo): validação do número de telefone que originou acomunicação e confirmação de informações de conhecimento pessoal do cliente.

N. Observação:

- Esse canal não é utilizado para serviços transacionais e tem uso permitido apenas através de plataforma corporativa que possui controles de segurança.
- Na utilização de mensagens de correio, a privacidade da informação deve ser preservada e a mensagem criptografada. Deve-se utilizar certificados que garantam a integridade da mensagem ou senhas em arquivos que devem ser transmitidas ao clientepor outro meio de comunicação.

Os canais de relacionamento também devem oferecer conteúdo educativo sobre precauções e cuidados a respeito de aspectos de segurança a fim de proteger acessos, contas e recursos dos clientes com a Desenvolve-AL.

10. PLANO DE RESPOSTAS A INCIDENTES

De acordo com a Resolução nº 4893, do Banco Central do Brasil, que dispõe sobre a política de Segurança Cibernética ,e as normas internas sobre o mesmo assunto da Desenvolve-Al, estaremos adotando as medidas sugeridas no Art. 3 da resolução:

- procedimentos e os controles para reduzir a vulnerabilidade da

instituição a incidentes ;

- controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
- registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;
- procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados pelos envolvidos no manuseio dos dados ou informações sensíveis da instituição;
- Classificação do tipo de incidente e da informação;
- implementação de programas de capacitação e de avaliação periódica de pessoal;
- informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e
- o comprometimento da alta administração com a melhoria contínua dos processos internos de gestão da informação.

A. Conceitos e Definições

- **ataque:** Evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
- ***bot***: Código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;
- **GMT**: *Greenwich Mean Time*, ou Horário Médio de Greenwich, baseado no primeiro meridiano de Greenwich, que passa pelo Observatório Real, perto de Londres.
- **IP**: Protocolo da Internet (*Internet Protocol*), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;
- **log**: Processo de registro de eventos relevantes num sistema computacional;
- **porta**: Programa de computador específico ou processo específico servindo de ponto final de comunicação em um sistema operacional hospedeiro de um outro dispositivo.
- ***scripts***: conjunto de instruções para que uma função seja executada em determinado aplicativo;

- **SLA**: Acordo de Nível de Serviço (do inglês *Service Level Agreement*);
- ***spam***: Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
- ***spyware***: Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;
- ***trojan***: Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;
- **vírus**: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;
- ***worm***: Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;
- ***DdoS:*** (*Distributed Denial of Service*) Incidente de Segurança da Informação capaz de degradar ou indisponibilizar sistemas, redes ou serviços;
- ***Ransomware:*** Código malicioso que torna inacessível os dados armazenados em um equipamento;

B. Fluxo para compartilhamento de informações de incidentes

C. Atores

Rev.	Revisão	Data da Revisão	Diretor Presidente	Data da Aprovação
03	(Eduardo Silva, Rogeno Portela, Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	06/06/2023

- **Superintendente de TI**: responsável pelas ações de segurança da informação que Identifica, avalia e define estratégias para o melhor desempenho.
- **Analista de TI**: responsável por coordenar toda infraestrutura de TI, implanta e presta suporte a sistemas de informação e soluções tecnologicas, definindo requisitos e especificando sua arquitetura. Instala e customiza sofwares com configurações e procedimentos de segurança de rede.
- **Assistente de TI**: restaura suporte aos usuários da rede de computadores, envolvendo a montagem, reparos e configurações de equipamentos e na utilização do hardware e software disponíveis. Prepara inventário do hardware existente e realiza a montagem dos equipamentos e implantação dos sistemas utilizados pelas unidades de serviço.
- **Desenvolvedor (programador)**; desenvolvimento de sistemas com manutenção e otimização de operações que envolvem o software de aparelhos eletrônicos, como o computador, smartphone, tablet, entre outros.
- **Ponto de contato**: responsável estratégico pela comunicação e ponto focal de contato da equipe de resposta a incidentes com outros setores da organização ou grupos externos.

D. Notificação de incidentes

Figura 1 . Tela do Sistema de Chamado técnico e Incidentes

Figura 2 . Tela de acompanhamento dos chamados

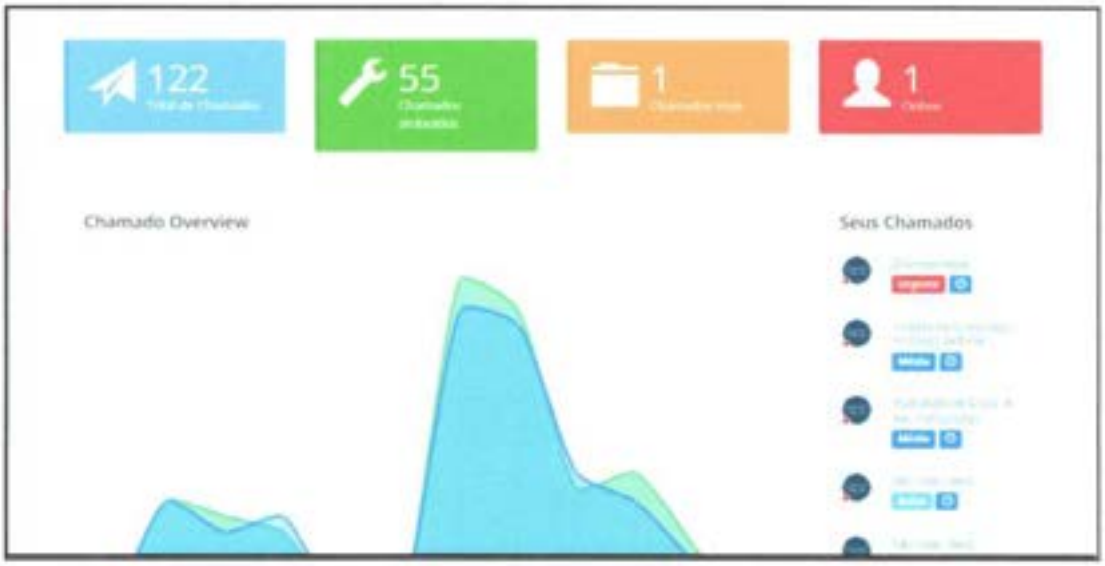


Figura 3 . Tela da timeline dos chamados

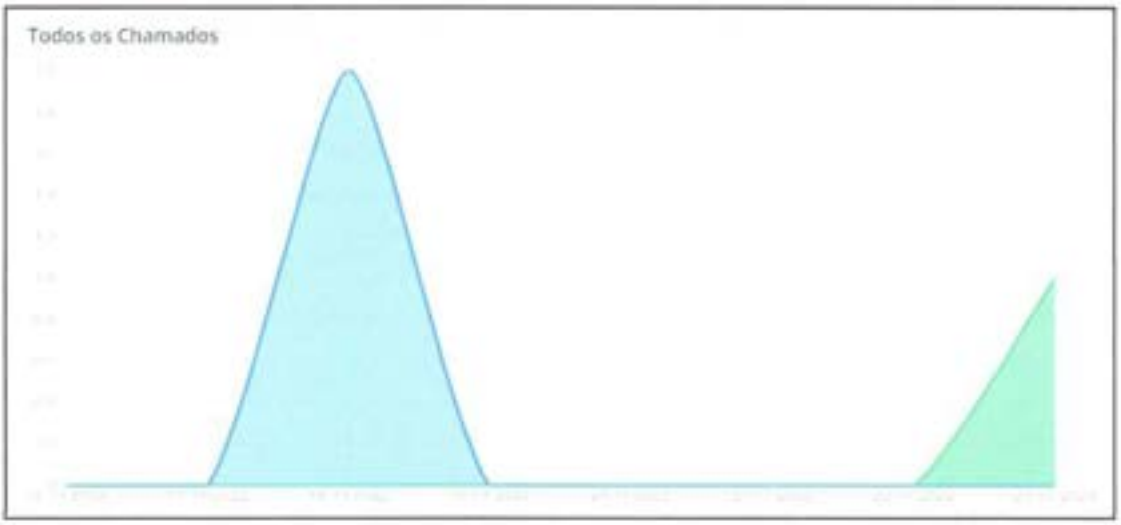
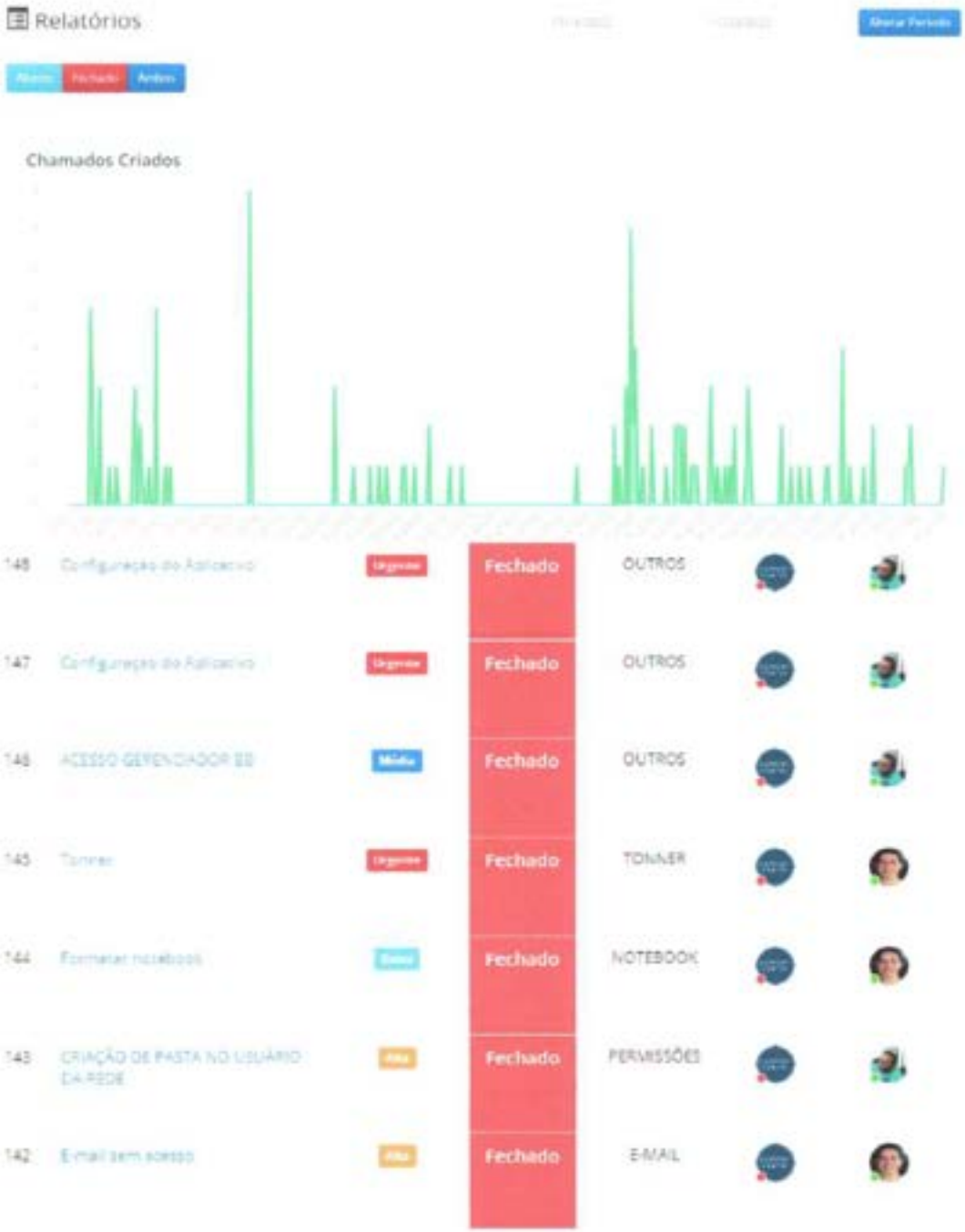


Figura 4 . Tela do controle geral dos chamados e incidentes



Rev.	Revisão	Data da Revisão	Diretor Presidente	Data da Aprovação
03	(Eduardo Silva, Rogerio Portela, Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

E. INCIDENTES DE PRIVACIDADE DE DADOS

O encarregado de dados da Desenvolve – Agência de Fomento de Alagoas será o canal de comunicação para notificar os incidentes de privacidade.

Encarregado pelo tratamento de dados:
Superintente de TI
Telefone: (82) 3315-3468
E-mail: ti@desenvolve-al.com.br

Endereço:
Rua Deputado José Lagés, 972 Ponta verde
CEP 57035-330 Maceió
- AL

Para incidente com vazamento de dados pessoais, o Encarregado de Dados deve avaliar e fazer as comunicações, bem como informar e subsidiar os controladores ou operadores do sistema. Essas comunicações devem incluir ao notificador, informações para os titulares de dados, relatórios formais para a Autoridade Nacional de Proteção de Dados (ANPD).

F. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E FLUXO DO PROCESSO

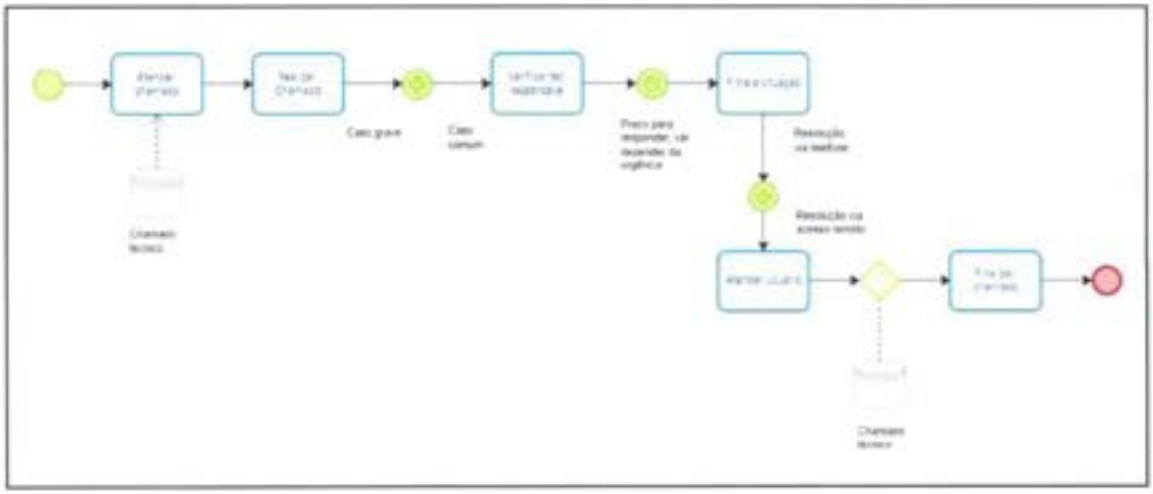
Quanto às notificações de incidentes de segurança da informação, serão utilizado o meio comunicação institucional: e-mail para o setor de compliance.

Encarregado pelo tratamento de dados:
Analista de TI
Telefone: (82) 3315-3468
E-mail: ti@desenvolve-al.com.br
Endereço:
Rua Deputado José Lagés, 972 Ponta verde
CEP 57035-330 Maceió
- AL

2º - Canal para pessoa com vínculo ativo com a Desenvolve-AL:

Serviço gerenciador de serviços de tecnologia da Informação (CHAMADO TÉCNICO e INCIDENTES), Endereço do sistema:
http://10.32.4.188/chamado/
Caminho no sistema: "Segurança da Informação" >> "Notificações de Problemas de Segurança" >> "Relatar Problemas de Segurança"

- **Fluxograma do Processo do registro do Incidente:**



G. PADRÕES DE NOTIFICAÇÃO

Ao se registrar uma notificação de incidente de segurança da informação eprivacidade, devem-se inserir as seguintes informações:

1. **Origem do incidente:** unidade, setor ou organização à qual dispositivo ou o processo que originou o incidente pertence;
2. **Contato da origem:** e-mail, telefone ou outro contato disponível do informante do incidente;
3. **Registro do tempo da ocorrência do incidente:** data e hora em formato GMT na qual o incidente foi identificado. Exemplo: "10:23, 20 de Março de 2023";
4. **Local onde originou o incidente:** endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente;
5. **Recursos utilizados pela origem do incidente:** especificação do tipo do protocolo (IP, TCP, UDP, etc.) e portas, ou procedimentos operacionais, adotados na ação do incidente;
6. **Endereço do alvo:** endereço IP (IPv4 ou IPv6) do dispositivo ou endereço de acessodo serviço que foi o alvo do incidente;
7. **Protocolos e portas alvos do incidente:** especificação do tipo do protocolo (IP,TCP, UDP, etc.) e portas utilizados no destino do incidente;
8. **Serviços envolvidos:** especificação do serviço que foi alvo do incidente (http, ftp, smtp, etc.) e versões de sistemas utilizados;
9. **Descrição do incidente:** breve descrição do incidente, tais como tipo do ataque,motivação aparente, ou outras características relevantes;

10. **Logs ou evidências:** anexação das porções de log, imagens, códigos de erro ououtros registros que evidenciem a ocorrência do incidente;

H. REGISTRO DO INCIDENTE

Utilização do software de registro de chamadas de suporte técnico CHAMADO TÉCNICO para registrar e catalogar o incidente (http://10.32.4.188/chamado/). O incidente é documentado em base de conhecimento apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

I. TRIAGEM DO INCIDENTE

O objetivo do processo de triagem é reunir informações sobre o incidente, avaliar a sua natureza, e classificá-lo como incidente para que, adiante, se inicie o processo de tratamento.

Fluxograma: "Incidente não classificado" >> "Triagem do Incidente" >> "Classificar tipo de Incidente" >> "Definir Criticidade" >> "Alterar Situação do Incidente" >> "Incidente Classificado".

J. CLASSIFICAÇÃO DO INCIDENTE

Classificar o incidente deixa claro o tipo de atendimento requerido e ajuda a definir sua criticidade.

1. **Conteúdo abusivo:** spam, assédio, etc;
2. **Código malicioso:** bot, worm, vírus, trojan, spyware, scripts;
3. **Prospecção por informações:** varredura, sniffing, engenharia social;
4. **Tentativa de intrusão:** tentativa de exploração de vulnerabilidades, tentativa deacesso lógico;
5. **Intrusão:** Acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação;
6. **Indisponibilidade de serviço ou informação:** negação de Serviço, sabotagem;
7. **Segurança da informação:** acesso não-autorizado à informação, modificação nãoautorizada da informação;

8. **Fraude:** violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
9. **Outros:** incidente não categorizado.

K. CRITICIDADE DO INCIDENTE

Definir uma ordem de atendimento dos incidentes e um SLA de acordo com a urgência de tratamento e o impacto nas áreas de negócio da UFLA. Determinar a classificação de criticidade do incidente de acordo com as classificações:

1. **Alto (Impacto Grave)** Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;
2. **Médio (Impacto Significativo)** Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição;
3. **Baixo (Impacto Mínimo)** Possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

L. SITUAÇÃO DO INCIDENTE

Definir uma situação para cada incidente, a fim de acompanhar o andamento do mesmo dentro do processo de tratamento.

1. **Aberto:** Nesse momento foi realizado apenas o registro das informações;
2. **Processando:** Quando o chamado é assumido por um técnico e está em tratamento;
3. **Pendente:** É preciso confirmar alguma informação com o solicitante antes dedar prosseguimento. Tentativas de contato devem ser realizadas e registradas;
4. **Pendente de Terceiros (Transferido):** Ocorre quando uma equipe solucionadoranão tem ação no chamado e é repassado para outra coordenadoria ou equipe;
5. **Solucionado:** Indica que o procedimento técnico foi aplicado e aparentementeo chamado foi solucionado;
6. **Fechado:** Quando a solução do chamado foi confirmada pelo solicitante.O fechamento pode ocorrer automaticamente ou por contato.

M. PRESERVAÇÃO DE EVIDÊNCIAS

Antes de se iniciar as ações para restaurar as operações do ambiente, é necessária a preservação de provas para a identificação correta da causa raiz do incidente e, posteriormente, para a recuperação dos sistemas afetados.

N. PROCESSO DE MITIGAÇÃO DO INCIDENTE

Preparação: gerenciar as ferramentas para análise de incidentes, incluindo oconhecimento de todo o ambiente utilizado;

a. Implementar mecanismos de defesa e controle de ameaças;
b. Desenvolver procedimentos para lidar com incidentes de forma eficiente;
c. Obter recursos e equipe necessária para lidar com os problemas;
d. Estabelecer infraestrutura de suporte à atividade de resposta a incidentes.

Detecção: detectar o incidente, determinar o escopo e as partes envolvidas com o incidente;

e. Identificar todos os sistemas e serviços afetados relacionados com o incidente;
f. Avaliar o impacto do incidente e os potenciais riscos dos sistemas afetados (dados vazados, informações de instituições parceiras, impacto na própria organização e impacto na reputação);
g. Identificar a existência de outros eventos e alertas relacionados com o incidente em questão;
h. Identificar que tipo de informação e processos podem ter sido afetados;
i. Identificar os responsáveis pelo sistema comprometido, equipes de suporte e donos das informações.

Contenção: conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos.

j. Desconectar o sistema comprometido ou isolar a rede afetada;
k. Desativar o sistema para evitar maiores perdas quando há perda ou roubo de

informações durante o ataque;

l. Alterar políticas de roteamento dos equipamentos de rede ou bloquearpadrões de tráfego, interrompendo o fluxo malicioso;

m. Desabilitar serviços vulneráveis, inibindo comprometimento de outrossistemas.

Erradicação: eliminar as causas do incidente, removendo todos os eventosrelacionados.

n. Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;

o. Assegurar a remoção de todos os métodos de acesso utilizados pelo atacante: novas contas de acessos; backdoors e, se aplicável, acesso físico ao sistema comprometido, etc.

Recuperação: restaurar o sistema ao seu estado normal.

p. Caso exista Plano de Continuidade de Negócio dos serviços impactados, elesdevem ser iniciados, conforme especificado no respectivo plano.

q. Restaurar a integridade do sistema;

r. Garantir que o sistema foi recuperado corretamente e que as funcionalidadesestejam ativas;

s. Implementar medidas de segurança para evitar novos comprometimentos;

t. Restauração do último e íntegro backup completo armazenado.

Avaliação: avaliar as ações realizadas para resolver o incidente, documentandodetalhes, e discutir lições aprendidas.

u. Caracterizar o conjunto de lições aprendidas de modo a aprimorar osprocedimentos e processos existentes;

v. Identificar características de incidentes que podem ser utilizadas para treinar novos membros da equipe;

w. Prover estatísticas e métricas relativas ao processo de resposta a incidentes;

x. Obter informações que podem ser utilizadas em processos legais.

O. FECHAMENTO DO INCIDENTE

Planilha de Controles Operacionais e Incidentes:

Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto.	05/06/2023

Uma planilha elaborada em Microsoft Excel, é elaborada (Figura 5) com os Incidentes e as soluções adotadas bem como triagem,classificação , criticidade , situação e mitigação adotada.

Figura 5 . Tela da Planilha do resumo dos incidentes.

- Controle dos Incidentes:

Figura 6 . Tela da Planilha do resumo dos incidentes por mês.

PLANILHA DE CONTROLE DOS INCIDENTES.

Responsável de TI	Nº do Chamado aberto	Data /Hora	Ocorrência (Registro)	Análise de Causa	Impacto para Agência	Ações Realizadas	Controle de Efeitos	Observações
Valdick - Superintendente de TI / Eduardo - Analista de TI	CPJ. 931.	28/10/2022	FIBRA-INTERNET (ROMPIMENTO)	TRECHO DA FIBRA, AFETANDO VARIOS ORGÃOS EM UM TRECHO DA VIA	ESTAMOS UTILIZANDO A CONTIGÊNCIA DO LINK DE INTERNET	FOI ABERTO UM CHAMADON NO ITEC - INSTITUTO E TECNOLOGIA EM INFORMÁTICA E INFORMAÇÃO).	EM COMUNICAÇÃO COM O SUPORTE, ESTA PREVISTO O RETORNO NO MESMO DIA.	CORREÇÕES NO DECORRER DO DIA, FOI CONCLUÍDO COM SUCESSO.

MAIO 2022 | JUNHO 2022 | JULHO 2022 | AGOSTO 2022 | SETEMBRO 2022 | OUTUBRO 2022

P. RECOMENDAÇÕES E RESPOSTA AO INCIDENTE

Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto.	05/06/2023

Havendo recomendações a serem feitas aos usuários, administradores de sistemas ou a outras equipes de segurança, estas devem ser feitas no processo de fechamento do incidente.

Q. LIÇÕES APRENDIDAS

Consiste em se avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas. Devem-se relacionar e documentar no chamado do incidente as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões. A partir da mitigação do incidente e sua resolução, deve ser conduzido o apanhado de lições aprendidas, com outros atores se necessário, com o objetivo de discutir erros e dificuldades encontradas na mitigação do evento ocorrido, propor melhoria na infraestrutura computacional e para os processos de resposta a incidentes.

A área afetada deve ser comunicada das decisões tomadas para prevenção de incidentes da mesma natureza, caso se tenha consenso de implementar melhorias na infraestrutura de segurança.

11. ANÁLISE E GERENCIAMENTO DOS RISCOS

Os riscos desta politica são analisados e avaliados a partir dos eventos que possam proporcionar ameaças ou ocasionar perdas. As análises realizadas proporcionam as estratégias para eliminar e/ou amenizar estes riscos, conforme mencionado no item 5 desta politica.

A avaliação de risco considera, ainda, os impactos do tipo socioambiental, operacional, financeiro, as oportunidades de negócio, o cumprimento dos prazos e os requisitos legais.

De acordo com a Resolução nº 4893, do Banco Central do Brasil, que dispõe sobre a politica de Segurança Cibernética ,e as normas internas para interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem utilizados, estaremos adotando as medidas do Art. 20 da resolução:

A. Ações para mitigar os efeitos dos incidentes;

Os incidentes que utilizam a tecnologia da informação podem ter repercussões extremamente negativas tanto para as organizações quanto para os individuos afetados. Para lidar com esses impactos, são necessárias atividades proativas e reativas para limitar os danos, restaurar o desempenho normal dos sistemas e prevenir futuros acidentes. As ações para mitigação dos efeitos dos incidentes que serão adotadas:

Resposta imediata: Assim que um incidente é identificado, é fundamental tomar medidas imediatas para limitar o problema e reduzir os seus efeitos. É possível que isso exija pausar os serviços afetados, isolar computadores comprometidos ou desconectar dispositivos vulneráveis da rede.

Análise do Impacto: É fundamental, uma vez controlada a crise, realizar um estudo exaustivo do impacto causado. Avaliar os locais afetados, determinar quais dados foram comprometidos, avaliar a quantidade de danos e, se possivel, quantificar as perdas fazem parte desse processo. Usar esta pesquisa para ajudar a determinar as prioridades de recuperação será benéfico.

Restauração do serviço: quando um incidente foi contido e seu impacto avaliado, é hora de iniciar o processo de restauração de sistemas e serviços danificados. Isso pode envolver a restauração de backups de dados, eliminação de malware, correção de vulnerabilidades de segurança e implementação de etapas para evitar ocorrências de natureza semelhante no futuro.

A comunicação e a notificação: são essenciais, pois é necessário fornecer informações sobre o incidente e suas consequências para todos da instituição, bem como todos que têm interesse no assunto. Isso inclui parceiros, fornecedores, órgãos reguladores e, potencialmente, o público em geral, dependendo da natureza e abrangência da ocorrência. Construir confiança dentro da instituição e mitigar os danos que podem ser causados à sua reputação se beneficiam de uma comunicação aberta e honesta.

Avaliação das lições aprendidas: É essencial realizar uma investigação pós-evento após a resolução de um incidente para determinar as causas subjacentes do problema, as vulnerabilidades que foram exploradas e as áreas que precisam ser aprimoradas. Os sistemas de segurança serão beneficiados com as lições aprendidas, o que ajudará a reforçá-los e prevenir futuros acidentes.

O melhoramento contúnuo da segurança das informações Proteger dados confidenciais é um esforço contínuo. Para que a instituição permaneça resiliente diante dos perigos em constante evolução, suas políticas, processos e controles de segurança devem ser avaliados e atualizados rotineiramente. Isso implica fornecer treinamento ao pessoal, implementar medidas de segurança adicionais e realizar auditorias frequentes para garantir a conformidade com os padrões de segurança.

Se faz necessário uma abordagem criteriosa e permanente para garantir a segurança dos sistemas e dados. É imperativo praticar a prevenção e a prontidão para diminuir os efeitos dos eventos e facilitar uma recuperação rápida.

B. Prazo para retorno das atividades.

A duração do retorno às atividades após um evento de tecnologia da informação pode variar muito com base no tipo e gravidade do incidente, na complexidade dos sistemas afetados e nas técnicas de recuperação empregadas. Não existe um prazo específico que se aplique a todas as situações, pois cada incidência é única.

Alguns pequenos incidentes podem ser resolvidos e as atividades podem reiniciar em algumas horas. Por exemplo, se um determinado servidor tiver uma falha isolada, pode ser fácil substitui-lo por um servidor de backup e restaurar a funcionalidade em um curto período de tempo.

No entanto, ocorrências mais catastróficas, como ataques cibernéticos extensos, violações de dados em larga escala ou falhas criticas de infraestrutura, podem exigir uma investigação completa, reconstrução de sistemas e adição de medidas extras de segurança. Nesses casos, o tempo de recuperação pode levar dias, semanas ou até meses.

Além disso, é vital examinar aspectos adicionais que podem afetar o tempo de resposta, como disponibilidade de recursos, complexidade dos sistemas afetados, capacidade de recuperar dados de backups confiáveis e colaboração com terceiros, como fornecedores e parceiros.

Essas estratégias devem levar em consideração a complexidade dos sistemas e processos envolvidos, bem como expectativas realistas de recuperação, no entanto, estaremos adotando as regras abaixo:

Incidentes menores: O tempo de resposta para incidentes menores pode variar de algumas horas a dois dias ou mais. Exemplos de eventos menores incluem falhas isoladas do sistema, problemas de conexão limitada ou defeitos de software especializados. Esses problemas geralmente têm uma solução rápida, que envolve a substituição ou o reparo do componente danificado.

Incidentes moderados: O tempo de resposta para incidentes que incluem sistemas mais complicados ou afetam vários locais, como violações de segurança localizadas, malware que se espalhou para várias máquinas ou interrupções de serviços essenciais específicos, o tempo de resposta pode variar de alguns dias a uma semana. Essas ocorrências incluem violações de segurança localizadas, malware que se espalhou para várias máquinas ou interrupções de serviços críticos específicos. Nessas circunstâncias, é vital avaliar a extensão do problema, tomar medidas de recuperação e garantir que os sistemas sejam restaurados com segurança.

Incidentes graves : Quando se trata de incidentes significativos, como ataques cibernéticos sofisticados, violações massivas de dados ou amplas falhas de infraestrutura, o tempo de resposta pode levar de várias semanas a vários meses. Essas ocorrências exigem uma resposta completa, que pode envolver cooperação com terceiros, realização de investigações forenses, reconstrução de sistemas, restauração de dados de backups confiáveis, adoção de medidas extras de segurança e muito mais.

Os prazos aqui listados são apenas uma referência geral e podem ser ajustados de

acordo com as particularidades de cada ocorrência. É absolutamente necessário ter um plano de resposta a incidentes bem desenvolvido e ajustado que inclua planos de continuidade de negócios para direcionar as operações e definir cronogramas aceitáveis para o reinicio das atividades após um incidente envolvendo a tecnologia da informação.

C. Comunicação do Incidente

Após a ocorrência de um evento envolvendo tecnologia da informação na instituição, é imprescindível uma comunicação adequada e transparente com todos os principais atores da gestão da empresa, parceiros e clientes, se for o caso. A seguir apresentamos os atores que deverão ser informados:

Comitê de Gestão Integrada de Riscos Cibernéticos: É imperativo que, assim que um problema for descoberto, um membro da comunidade de segurança da informação, um membro do departamento de tecnologia da informação e um membro da alta administração sejam notificados imediatamente. Este grupo se encarregará de organizar as diversas ações referentes aos esforços de reação, investigação e recuperação.

Gerência e Alta Administração: O incidente precisa ser relatado imediatamente à gerência de onde o incidente ocorreu e à Diretoria Executiva da Desenvolve-AL (formada pelo Presidente e Diretores operacionais), especialmente se tiver um efeito substancial nas operações, segurança de dados ou reputação da organização. Para que possam fornecer o nível adequado de direção e tomar decisões estratégicas, eles precisam ser informados sobre a situação.

Gerência de Comunicações: A gerência de Comunicações deve ser envolvida para coordenar a comunicação com o mundo exterior em relação ao incidente, caso seja necessário. Isso abrange a preparação de comunicados à imprensa, bem como a resposta a consultas de clientes, parceiros e fornecedores, além de outras partes interessadas externas.

Equipe de TI e administradores de sistema: A equipe interna de TI, incluindo administradores de sistema e especialistas em segurança, deve ser informada para auxiliar na investigação, mitigação do incidente e implementação de medidas de segurança adicionais. Isso inclui informar a equipe de TI para ajudar a mitigar a situação.

Funcionários que podem ser afetados: È fundamental comunicar-se com os funcionários que podem ser afetados por um incidente, para que eles estejam cientes das circunstâncias e possam responder adequadamente seguindo as instruções dadas. Isso é especialmente importante em situações em que houve violação de dados ou se é necessário fazer uma modificação nos procedimentos ou processos de trabalho.

Autoridades e órgãos reguladores: Pode ser necessário informar as autoridades ou órgãos reguladores apropriados em algumas circunstâncias, dependendo da natureza da ocorrência, bem como das leis e regulamentos aplicáveis. Este pode ser o caso quando for necessário fazê-lo. Isso abrange coisas como agências de proteção de dados no caso de violação dos dados pessoais dos indivíduos, bem como ao ITEC – Instituto de Tecnologia do Estado de Alagoas, o Tribunal de Contas do Estado, e ao Banco Central do Brasil

È fundamental observar que a comunicação precisa ser cuidadosamente planejada e gerenciada, levando em consideração as exigências legais, as normas internas da Agência e os interesses das partes envolvidas. Manter a confiança das partes interessadas requer um alto nível de transparência, bem como comunicação antecipada, a fim de reduzir os efeitos negativos do incidente

D. Providências adotadas para reinício das atividades;

Após a ocorrência do incidente, é necessário realizar uma série de procedimentos necessários para que as atividades possam ser retomadas de forma segura e eficaz:

Avaliação dos Sistemas Afetados: É importante realizar uma análise detalhada de todos os sistemas afetados pelo incidente. Se faz necessário determinar quais sistemas

foram comprometidos, quais dados podem ter sido perdidos ou comprometidos e a quantidade de danos causados. Desta maneira será mais fácil priorizar as ações de recuperação e tomar as ações corretivas apropriadas.

Limpeza e restauração: se o incidente incluir malware ou sistemas comprometidos, é vital executar uma limpeza completa em todos os sistemas afetados e restaurá-los ao seu estado original. Pode ser necessário reinstalar sistemas operacionais, aplicativos e outros softwares, bem como recuperar dados de backups confiáveis.

Implementar precauções de segurança adicionais: É essencial, uma vez que os sistemas tenham sido restaurados, implementar precauções de segurança adicionais para evitar incidentes no futuro. Isso pode incluir a execução de atualizações de software e sistema operacional, instalação de patches de segurança, avaliação de regras de segurança, adoção de autenticação multifator e segmentação de redes, entre várias outras ações apropriadas.

Teste e verificação: antes de retomar as operações normais, é essencial realizar testes e verificações para confirmar que todos os sistemas estão operando adequadamente e que quaisquer vulnerabilidades que possam estar presentes foram corrigidas. Será necessário realizar os testes de segurança e desempenho, bem como verificações para garantir que os controles de segurança apropriados foram instalados e estão funcionando conforme o esperado.

Comunicação interna: É importante manter o pessoal informado sobre a ocorrência, as ações que foram tomadas e quaisquer medidas extras de segurança que foram implementadas. É importante garantir que todos estejam cientes das novas precauções e que possam contribuir para a segurança geral dos sistemas, portanto, é importante fornecer orientações claras sobre quaisquer modificações que sejam feitas nos processos e políticas de segurança. Se necessário, treinamento também deve ser fornecido.

Monitoramento contínuo: Uma vez retomadas as operações, é fundamental implantar um sistema capaz de monitorar continuamente, a fim de identificar possíveis perigos e futuros acidentes. Monitore a rede, os logs do sistema e os padrões de tráfego, bem como faça uso de ferramentas de detecção de intrusão, a fim de identificar atividades potencialmente maliciosas e reagir prontamente a qualquer ocorrência incomum.

12. ROTINAS DOS SISTEMAS:

	SISTEMAS			
ROTINAS	**Antivírus**	**Firewall**	**Backup e Restore**	**Corporativo De Crédito**
Periodicidade	Em tempo real	Em tempo real	Diário, Semanal, Mensal e Anual	Em tempo real
Atualização Software	Diária	N/A	N/A	Mensal
Atualização Regras	N/A	Novos objetos, usuários e/ou Policy	Novos agendamentos e/ou clients	Novas regras de negócio da Agência
Gerenciamento	Console	Console	Console	N/A
Hardware	Hyper-V	Redundante (contigência)	Hyper-V e Tape Drive	Redundante
Plano de Continuidade Operacional	Licenciamento com fabricante	Em renovação	Equipamento em garantia com o fabricante	Ambientes de Produção, Contingência e Homologação
Suporte	Equipe TI e fabricante	Equipe TI e fabricante	Equipe TI e fabricante	Equipe TI e fabricante
Relatórios Gerenciais	Sim	Sim	Sim	Sim
Relatórios Operacionais	Sim	Sim	Sim	Sim
Base de Testes nível gerencial	N/A	N/A	N/A	Sim
Base de Testes nível usuário	N/A	N/A	N/A	Sim
Administração de Usuário	Sim	Sim	Sim	Sim

13. SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENDO DE DADOS EM NUVENS

Para a contratação de qualquer serviços de tecnologia da informação, a mesma se dara com o processo contigênciado com uma base intalada na agência e a outra nas nuvens do ITEC (Instituto de Tecnologia em Informática e Informação do Estado de Alagoas). A situação atual nossa dos sistemas em andamentos, estão em nossos servidores), e a contigência esta nas nuvens do ITEC (Instituto de Tecnologia em Informática e Informação do Estado de Alagoas) Visando estabelecer critérios de segurança e aderência às eventuais legislações e regulações vigentes, foi desenvolvido na contratação das nuvens, existe uma aplicação com um banco de dados hospedado em nuvens, com a ulização do recurso, estamos com três maquianas virtuais, sendo uma de produção e duas para contigências.

O reinicio é automático, ITEC (Instituto de Tecnologia em Informática e Informação do Estado de Alagoas), nos que prove os serviços em nuvens, é o nosso espelhamento através de processos em redes, isso se dará de forma automática.

14. FIREWALL:

O Firewall utilizado na Desenvolve, é um equipamento com soluções de segurança integrada (UTM) que protege a rede contra-ataques unificados e ameaças avançadas. É um appliance com proteção integrada e em tempo real que integram as funcionalidades em uma plataforma de altissima performance, como:

- Unified Threat Management (UTM)
- Antispam
- Antivírus / Antispyware
- Controle de Aplicação
- Data Loss Prevention (DLP)
- Segurança de banco de dados
- Firewall

- Endpoint Protection
- Intrusion Prevention System (IPS)
- IPv6
- VoIP
- Virtual Private Network (VPN) – IPsec e SSL
- Segurança Virtual
- Vulnerabilidade e Gerenciamento de Conformidade
- Otimização de WAN
- Web Filtering
- Web Application Security
- Wireless LAN (WLAN)

O FortiGate Next Generation Firewall utiliza processadores de segurança especificos, serviços de segurança contra ameaças e a inteligência dos laboratórios FortiGuard para fornecer proteção de alto nivel e alto desempenho, incluindo tráfego criptografado. O FortiGate reduz a complexidade com visibilidade automatizada de aplicativos, usuários, rede e fornece classificações de segurança para adotar as melhores práticas de segurança recomendadas.

FIREWALL (NGFW)

Dispositivo de segurança de rede responsável pelo monitoramento, bloqueio ou permissão dos tráfegos de entrada e saída baseado num conjunto definido de regras de segurança.

15. COMUNICAÇÃO:

Mensalmente area de TI reportará a diretória e conselho de adminitração quando pertinente os status de incidencias ocorridas ou não, devrá ser enviada planilha: Controles Operacionais e Tentativas de Ataques Cibernéticos e Incidentes em anexo no e-mail.

A comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela agência, bem como das providências para o reinício das suas atividades sera realizada de imediato.

16. ANEXO: POLITICAS OPERACIONAIS E PROCEDIMENTOS OPERACIOANAIS:

14.1 - Planilha de Controles Operacionais e Tentativas de Ataques Cibernéticos;
14.2 - Controle dos Incidentes;
14.3 - Plano de Plano de Gestão de Incidentes de Segurança da Informação e Privacidade;
14.4 – Politica de Testes de Sistemas Informátizados;
14.5 – Plano de Continuidade de Negócio Tecnologia da Informação Rev. 02
11.6 - PO-STI-054-Backup e Restore

17. ANEXO:

Contratação de Serviços de Processamentos e Armazenamento de dados e de computação em Nuvem;

- ✓ Tela a tela dos servidores em nuvens abaixo:

- ✓ Tela de pagamento dos servidores em nuvens;

Summary By Project

Summary By Service

Atlas Instances

Atlas Data Storage

Atlas Data Transfer

Cloud Backup

Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

- ✓ Tela do Armazenamento Storage Local para Backup;

- ✓ Tela dos servidores instalados na estrutura em outro ambiente para contingência noITEC (Instituto de Tecnologia em Informática e Informação do Estado de Alagoas);

No site de contingência no Itec, estão instalados quatro Servidores Proliant BL460c Gen10, utilizando o Chassis c7000 do Itec – CloudSys002, nas Bays 13, 14, 15, 16, respectivamente

DESENVOLVE

✓ Tela das configurações dos 4 servidores instalados no ITEC;

Status | Information | Virtual Devices | Boot Options | IML Log

Device Information	
Blade Type	Server Blade
Manufacturer	HPE
Product Name	ProLiant BL460c Gen10
Part Number	863442-B21
System Board Spare Part Number	875625-001
Serial Number	BRC8249VT5
Serial Number (Logical)	
UUID	34333630-3234-5242-4338-323439565435
UUID (Logical)	00000000-0000-0000-0000-000000000000
BIOS Asset Tag	
System Name	DESITCFA01
ROM Version	I41 10/02/2018
Boot Mode	UEFI Optimized
Secure Boot	Disabled

- **Planilha de Controles Operacionais e Tentativas de Ataques Cibernéticos;**

Prezados, em atendimento ao item.10 da Política Cibernética da Agência de Fomento de Alagoas, ao qual, estabelece diretrizes, regras, e controles em todos os níveis da empresa, incluindo o gerenciamento dos riscos de Segurança da Informação, Segurança Cibernética e Incidentes. Sendo assim, informo através deste que no mês de janeiro 2023, ocorreram ataques cibernéticos. Abaixo, encaminho informações de controle.

- Controle dos Incidentes;

Prezados, em atendimento ao item.10 da Política Cibernética da Agência de Fomento de Alagoas, ao qual, estabelece diretrizes, regras, e controles em todos os níveis da empresa, incluindo o gerenciamento dos riscos de Segurança da Informação, Segurança Cibernética e Incidentes. Sendo assim, informo através deste que no mês de janeiro ocorreu incidente. Abaixo, encaminho informações de controle.

PLANILHA DE CONTROLE DOS INCIDENTES JANEIRO 2023								
Responsável de TI	Nº do Chamado aberto	Data /Hora	Ocorrência (Registro)	Análise de Cause	Impacto para Agência	Ações Realizadas	Controle de Efeitos	Observações
Valdick - Superintendente de TI / Eduardo - Analista de TI	114232	02/01/2023	FIBRA-INTERNET (ROMPIMENTO)	TRECHO DA FIBRA APRESENTOU VARIOS CRUZÕES EM UM TRECHO DA VIA	ESTAMOS UTILIZANDO A CONTINGÊNCIA DO LINK DE INTERNET	FOI ABERTO UM CHAMADO NO TEC - INSTITUTO E TECNOLOGIA EM INFORMATICA E INFORMAÇÃO	EM COMUNICAÇÃO COM O SUBORTE, ESTÃO AINDA PERCORRENDO TRECHOS PARA CORREÇÃO.	NÃO FOI CONCLUIDO

- **Plano de Plano de Gestão de Incidentes de Segurança da Informação e Privacidade;**

NOTIFICAÇÃO DE INCIDENTES

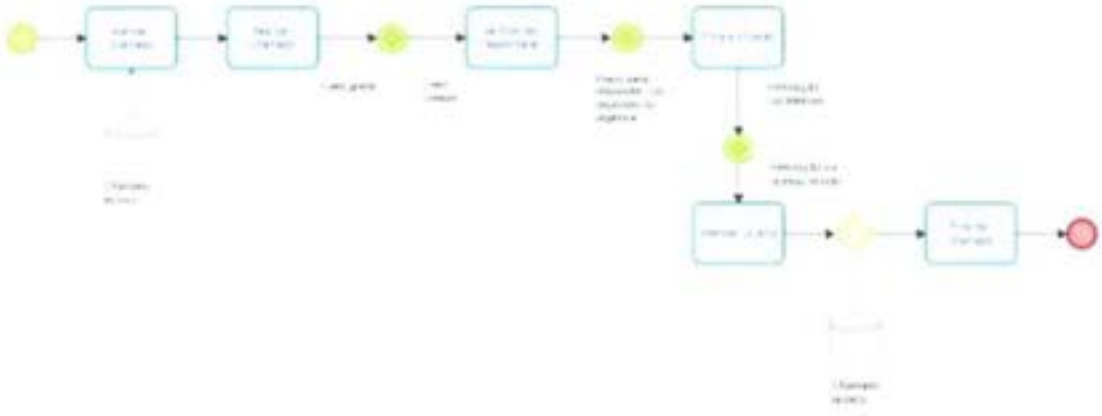
Figura 1 . Tela do Sistema de Chamado técnico e Incidentes

Figura 2 . Tela de acompanhamento dos chamados

Figura 4 . Tela do controle geral dos chamados e incidentes

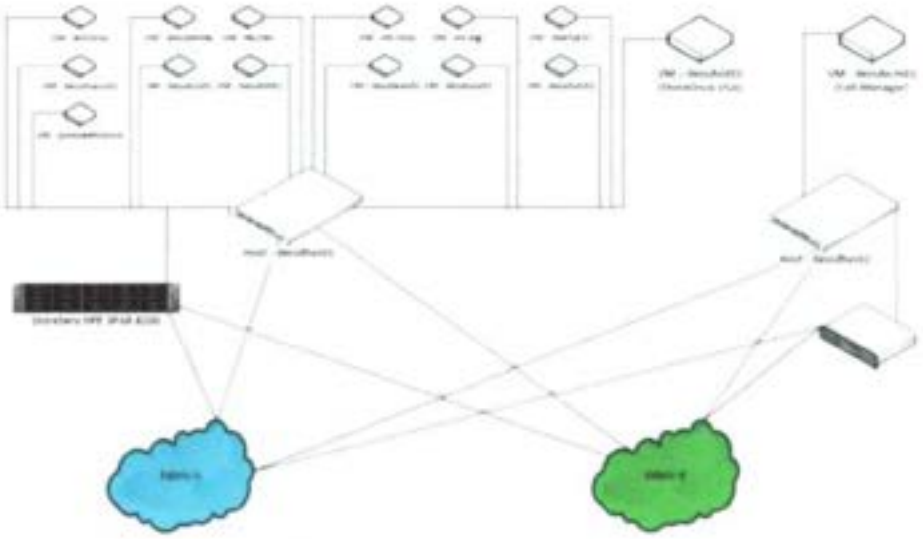
Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto.	05/06/2023

- **Fluxograma do Processo:**



- **PO-STI-054-Backup e Restore;**

Diagrama da Infraestrutura de Backup

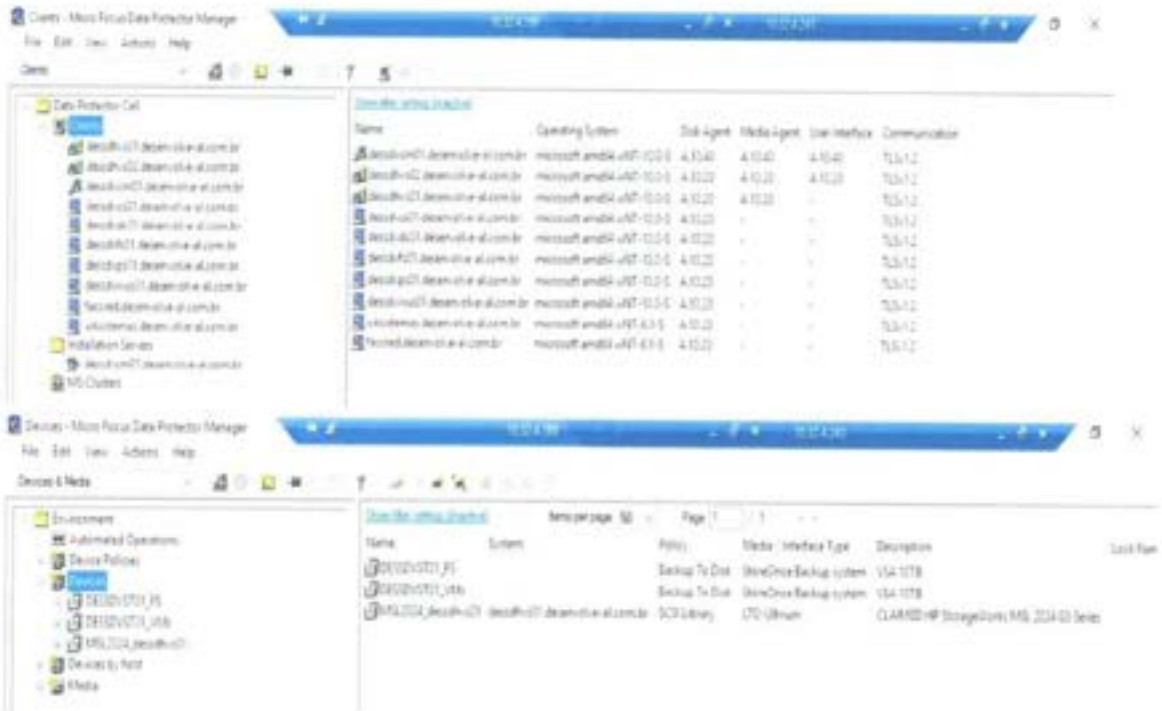


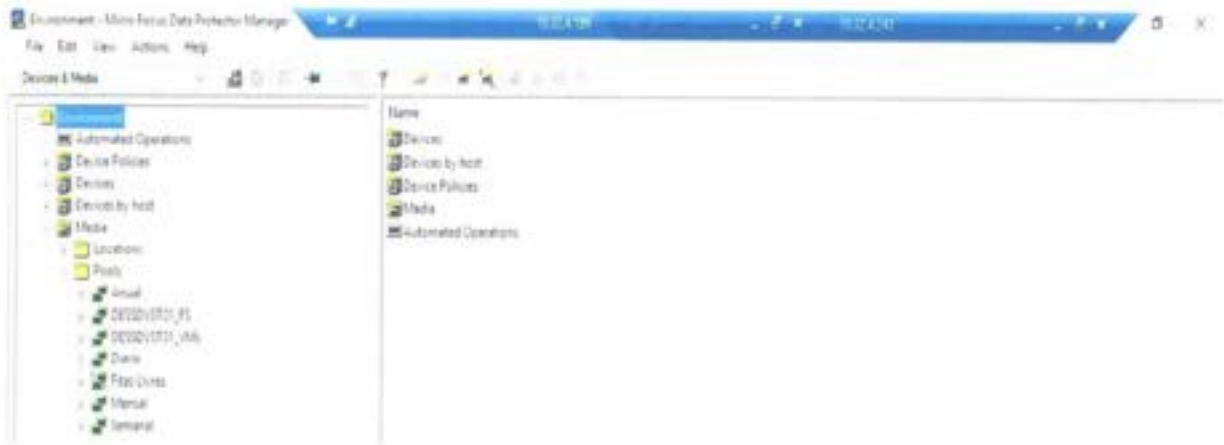
Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

Os clientes compreendem o Cell Manager e todas maquinas (fisicas ou virtuais), que estão com agente do Data Protector instalado, para realizar backup de file system.

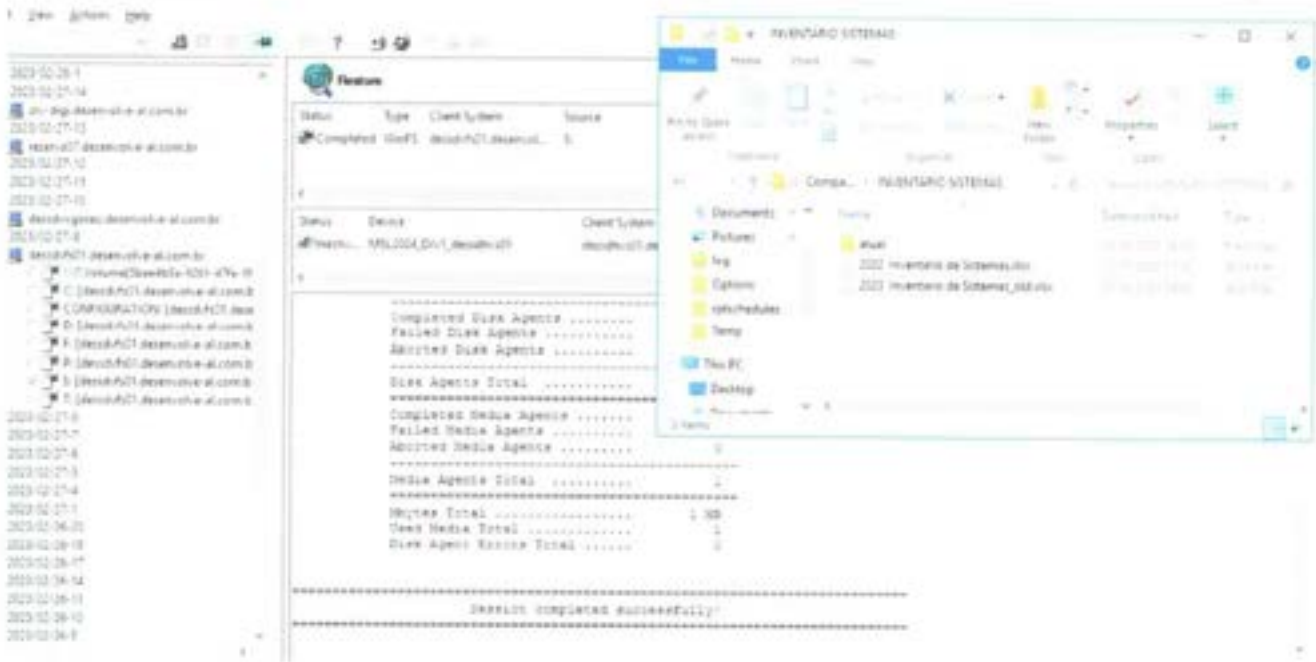
dessdvcm01.desenvolve-al.com.br
dessdhvs02.desenvolve-al.com.br
dessdhvs01.desenvolve-al.com.br
dessdvcs01.desenvolve-al.com.br
dessdvdc01.desenvolve-al.com.br
dessdvfs01.desenvolve-al.com.br
dessdvps01.desenvolve-al.com.br
dessdvwus01.desenvolve-al.com.br
wksistemas.desenvolve-al.com.br
faccred.desenvolve-al.com.br

- Data Protector Configurações Backups;





- Tela de Restauração de Backups:



Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto.	05/06/2023

- **Política de Testes de Sistemas Informátizados;**

  ✓ Links de Internet: 1 produção, 2 de contingência;

FO_ITEC (wan1)	Physical Interface
GVT (internal3)	Physical Interface
MPLS_ITEC (wan2)	Physical Interface

  ✓ Firewall;

  ✓ Alertas de Segurança:

Report Security Analysis - Desenvolve/AL-2023-02-26-0100

AT Alertas - TI
Para TI - Desenvolve

Desenvolve - Report Security Analysis-2023-02-26-0100_909.pdf
479 KB

These FortiAnalyzer reports have been subscribed with this mail address.
Please check the attachment.

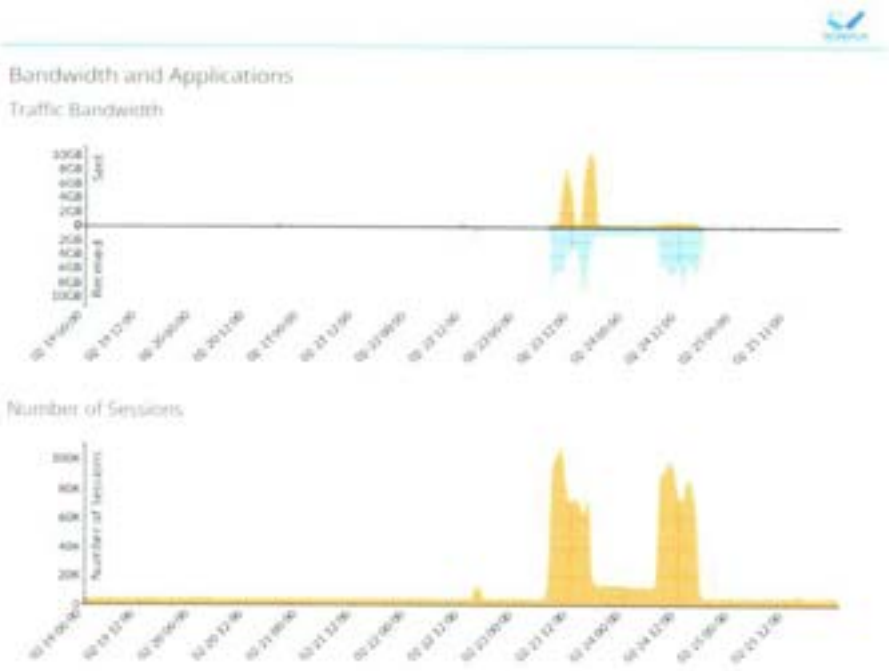
Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto.	05/06/2023

DESENVOLVE

FORTINET

Desenvolve - Report Security Analysis

- ✓ Largura de banda e suas aplicações;



- ✓ Categorias por largura de banda;

Rev.	Revisão	Data de Aprovação	Diretor - Presidente	Data de Aprovação
03	(Eduardo Silva; Rogerio Portela; Valdick Sales) - TI	05/06/2023	Eduardo Brasil Barreto	05/06/2023

DESENVOLVE

Top 20 Categories By Bandwidth

#	Category	Bytes
1	Information Technology	51.31 GB
2	Web based Applications	572.10 MB
3	Web Analytics	181.54 MB
4	Games	41.12 MB
5	Information and Computer Security	17.56 MB
6	Gambling	9.62 MB
7	Proxy Avoidance	5.32 MB
8	Alcohol	2.31 MB
9	Lingerie and Swimsuit	1.09 MB
10	Unrated	650.68 KB
11	Pornography	397.83 KB
12	Malicious Websites	282.55 KB
13	Potentially Unwanted Program	266.68 KB
14	Phishing	215.50 KB
15	Illegal or Unethical	62.65 KB
16	Newly Observed Domain	57.86 KB
17	Peer-to-peer File Sharing	33.51 KB

Top 50 Sites (and Category) by Bandwidth

#	Site	Category	Bytes
1	ac-[illegible]-shard-00-01.[illegible].mongodb.net	Information Technology	15.97 GB
2	appdesenvolve.nyc3.digitaloceanspaces.com	Information Technology	13.50 GB
3	au.download.windowsupdate.com	Information Technology	2.18 GB

✓ Tela mostrando com nenhuma ocorrência de Intrusos;

Threats

Malware Detected

Nenhuma correspondência para este relatório

Malware Victims

Nenhuma correspondência para este relatório

Malware Source

Nenhuma correspondência para este relatório

Botnet Detected

Nenhuma correspondência para este relatório

Botnet Victims

Nenhuma correspondência para este relatório

18. ARTEFATOS RELACIONADOS:

- https://bancoalfa.com.br/institucional/downloads/politicadesegurancadainformacao.pdf