RESOLUÇÃO Nº 318/2022

PALMAS, 27 DE JULHO DE 2022

Atualizar a Política de segurança Cibernética.

A DIRETORIA EXECUTIVA DA AGÊNCIA DE FOMENTO DO ESTADO DO TOCANTINS S/A, no uso de suas atribuições, e tendo em vista a atualização da política de segurança cibernética, aprovada em reunião de Conselho Administrativo em 30 de agosto de 2021.

RESOLVE:

Art. 1º Atualizar A Política de segurança cibernética, aprovada em reunião do Conselho de Administração;

Art.2º Esta resolução entra em vigor a partir desta data, revogando a resolução 216/2020.

DENISE ROCHA DOMINGUES
Diretora Presidente

JORGE LUIZ MATEUS
Diretor Operacional

Agência de FOMENTO do Estado do Tocantins

Coordenadoria de Tecnologia

POLÍTICA DE SEGURANÇA CIBERNÉTICA

RESPONSAVEIS:		
Tiago de Almeida Torres	63 3220-9824	tiago@fomento.to.gov.br

1 DEFINIÇÃO

O uso do termo “empresa” está em reverência à seguinte organização: Agencia de Fomento do Estado do Tocantins S.A;

2 INTRODUÇÃO

Esta Política de Segurança Cibernética se trata de um conjunto formal de regras pelas quais os stakeholders que possuem acesso à tecnologia da empresa e aos ativos de tecnologia da informação devem obedecer.

A política de segurança cibernética atende a vários propósitos. O objetivo principal é informar os usuários da empresa: funcionários, contratados, terceirizados, parceiros e outros usuários autorizados de seus requisitos obrigatórios para proteger os ativos de tecnologia e de informação da empresa. A política de segurança cibernética descreve os ativos de tecnologia e informações que devemos proteger e identifica muitas das ameaças a esses ativos.

A política de segurança cibernética também descreve as responsabilidades e os privilégios do usuário. O que é considerado uso aceitável? Quais são as regras relativas ao acesso à Internet? A política responde à essas perguntas, descreve as limitações do usuário e informa aos usuários que haverá penalidades por violação da política. Este documento também contém procedimentos para responder à incidentes que ameaçam a segurança dos sistemas de computadores e da rede da empresa.

3 O QUE PROTEGEMOS

É obrigação de todos os usuários dos sistemas da empresa proteger os ativos de tecnologia e de informação da empresa. Esta informação deve ser protegida contra acesso não autorizado, roubo e destruição. Os ativos de tecnologia e de informação da empresa são compostos pelos seguintes componentes:

- Hardware de computador, CPU, disco, e-mail, web, servidores de aplicativos, sistemas de computador, software aplicativo, software de sistema etc.
- É obrigação de todos os usuários dos sistemas da empresa proteger os ativos de tecnologia e de informação da empresa. Esta informação deve ser protegida contra acesso não

autorizado, roubo e destruição. Os ativos de tecnologia e de informação da empresa são compostos pelos seguintes componentes:

- Software de aplicação: usado pelos vários departamentos da empresa. Isso inclui aplicativos de software personalizados e pacotes comerciais de software prontos para uso.
- Hardware e software da Rede de Comunicações, incluído: roteadores, tabelas de roteamento, hubs, modems, multiplexadores, switches, firewalls, linhas privadas e software e ferramentas de gerenciamento de rede associados.

3.1 Classificação da Informação

As informações do usuário encontradas nos arquivos e bancos de dados do sistema do computador devem ser classificadas como confidenciais ou não confidenciais. A empresa deve classificar as informações controladas por eles. O CIO deve revisar e aprovar a classificação das informações e determinar o nível de segurança apropriado para melhor protegê-las. Além disso, o CIO deve classificar as informações controladas por unidades não administradas pelo CIO.

3.2 Classificação dos Sistemas de Informação

NÍVEL DE SEGURANÇA	DESCRIÇÃO	EXEMPLO
VERMELHO	Este sistema contém informações confidenciais que não podem ser reveladas a pessoas externas à empresa. Mesmo dentro da empresa, o acesso à essas informações, é fornecido na base de “necessidade de saber”. O sistema fornece serviços essenciais para a missão, vitais para à operação dos negócios. A falha deste sistema pode ter consequências potencialmente fatais e /	Servidor contendo dados confidenciais e outras informações do departamento em bancos de dados. Roteadores e firewalls de rede contendo tabelas de roteamento confidenciais e informações de segurança

	ou um impacto financeiro adverso nos negócios da empresa	
VERDE	Este sistema não contém informações confidenciais nem executa serviços críticos, mas fornece a capacidade de acessar sistemas VERMELHO através da rede.	PCs do departamento de usuários usados para acessar o servidor e o (s) aplicativo (s). Estações de trabalho de gerenciamento usadas por sistemas e administradores de rede.
BRANCO	Este sistema não é acessível externamente. Está em um segmento de LAN isolado, incapaz de acessar sistemas VERMELHO ou VERDE. Não contém informações confidenciais nem executa serviços críticos.	Um sistema de teste usado por projetistas de sistemas e programadores para desenvolver novos sistemas de computador.
PRETO	Este sistema é acessível externamente. Ele é isolado dos sistemas RED ou GREEN por um firewall. Enquanto realiza serviços importantes, não contém informações confidenciais	Um servidor da Web público com informações não confidenciais.

3.3 Local Area Network (LAN) Classificações

Uma LAN será classificada pelos sistemas diretamente conectados a ela. Por exemplo, se uma LAN contiver apenas um sistema VERMELHO e todos os usuários da rede estiverem sujeitos às mesmas restrições que os usuários do sistema VERMELHO systems. Uma LAN assumirá a Classificação de Segurança dos sistemas de nível mais alto anexados a ela.

4 DEFINIÇÕES

Externamente acessível ao público. O sistema pode ser acessado via Internet por pessoas de fora da empresa, sem um ID ou senha de logon. O sistema pode ser acessado via conexão dial-up sem fornecer um ID de logon ou senha. É possível "pingar" o sistema pela Internet. O sistema pode ou não estar por trás de um firewall. Um servidor da Web público é um exemplo desse tipo de sistema.

Não público, acessível externamente. Os usuários do sistema devem ter um ID de logon e senha válidos. O sistema deve ter pelo menos um nível de proteção de firewall entre sua rede e à Internet. O sistema pode ser acessado pela Internet ou pela Intranet privada. Um servidor FTP privado usado para trocar arquivos com parceiros de negócios é um exemplo desse tipo de sistema.

Apenas acessível internamente. Os usuários do sistema devem ter um ID de logon e senha válidos. O sistema deve ter pelo menos dois níveis de proteção de firewall entre sua rede e à Internet. O sistema não é visível para os usuários da Internet. Pode ter um endereço de Internet privado (não traduzido) e não responde à um "ping" da Internet. Um servidor Web de intranet privado é um exemplo desse tipo de sistema.

Chief Information Officer. O Coordenador do Departamento de Tecnologia da Informação (TI) atuará como Chief Information Officer (CIO).

Administrador de Segurança. Um funcionário de TI deve ser designado como Administrador de Segurança da Empresa.

5 Ameaças A Segurança

5.1 Funcionários

Uma das maiores ameaças de segurança são os funcionários. Eles podem causar danos aos seus sistemas, seja por incompetência ou de propósito. Faz-se necessário definir camadas de segurança para compensar isso também. Para atenuar a situação de ameaça, pode-se tomar as seguintes medidas:

- ✓ Somente dê direitos apropriados aos sistemas. Limitar o acesso apenas ao horário comercial.
- ✓ Não compartilhe contas para acessar sistemas. Nunca compartilhe suas informações de login com colegas de trabalho.

- ✓ Quando os funcionários são separados ou disciplinados, você remove ou limita o acesso aos sistemas.
- ✓ Avançado – Mantenha logs detalhados do Sistema em todas as atividades do computador.
- ✓ Proteja os ativos de computador com segurança física, de modo que somente funcionários com necessidades apropriadas possam acessar.

5.2 Hackers Amadores e Vândalos.

Essas pessoas são o tipo mais comum de invasores na Internet. A probabilidade de ataque é extremamente alta e também é provável que haja um grande número de ataques. Estes são geralmente crimes de oportunidade. Esses hackers amadores estão fazendo a varredura da Internet e procurando por falhas de segurança bem conhecidas que não foram conectadas. Servidores da Web e correio eletrônico são seus alvos favoritos. Uma vez que eles encontrem uma fraqueza, eles à explorarão para plantar vírus, cavalos de Tróia ou usar os recursos do seu sistema para suas intenções maliciosas. Se eles não encontrarem uma fraqueza óbvia, provavelmente passarão para um alvo mais fácil.

5.3 Hackers Criminosos e Sabotadores.

A probabilidade desse tipo de ataque é baixa, mas não é totalmente improvável, dada a quantidade de informações confidenciais contidas nos bancos de dados. A habilidade desses invasores é de médio a alto, já que eles provavelmente serão treinados no uso das mais recentes ferramentas de hackers. Os ataques são bem planejados e se baseiam em quaisquer pontos fracos descobertos que permitam a entrada na rede.

6 Responsabilidade do usuário

Esta seção estabelece a política de uso dos sistemas de computadores, redes e recursos de informações do escritório. Refere-se a todos os funcionários e contratados que usam os sistemas de computadores, redes e recursos de informações como parceiros de negócios e indivíduos que recebem acesso à rede para fins comerciais da empresa.

6.1 Uso Aceitável

As contas de usuário nos sistemas de computadores da empresa devem ser usadas apenas para os negócios da empresa e não devem ser usadas para atividades pessoais. O uso não autorizado do sistema pode estar violando a lei, constitui roubo e pode ser punido por lei. Portanto, o uso não autorizado do sistema de computação e das instalações da empresa pode constituir motivo para processo civil ou criminal.

Os usuários são pessoalmente responsáveis por proteger todas as informações confidenciais usadas e / ou armazenadas em suas contas. Isso inclui seus IDs de logon e senhas. Além disso, eles estão proibidos de fazer cópias não autorizadas de tais informações confidenciais e / ou distribuí-las a pessoas não autorizadas fora da empresa.

Os usuários não devem se envolver de propósito com à intenção de: assediar outros usuários; degradar o desempenho do sistema; desviar recursos do sistema para seu próprio uso; ou obter acesso a sistemas da empresa para os quais não possuem autorização.

Os usuários não devem se envolver de propósito com à intenção de: assediar outros usuários; degradar o desempenho do sistema; desviar recursos do sistema para seu próprio uso; ou obter acesso a sistemas da empresa para os quais não possuem autorização.

Os usuários são obrigados a relatar quaisquer deficiências na segurança do computador da empresa, qualquer incidente de uso indevido ou violação desta política ao seu supervisor imediato.

6.2 Uso da Internet

A empresa fornecerá acesso à Internet a funcionários e contratados conectados à rede interna e que tenham uma necessidade comercial para esse acesso. Funcionários e contratados devem obter permissão de seu supervisor e registrar uma solicitação com o Administrador de Segurança.

A Internet é uma ferramenta de negócios para a empresa. Ele deve ser usado para fins relacionados a negócios, como: comunicação via correio eletrônico com fornecedores e parceiros de negócios, obtenção de informações comerciais úteis e tópicos técnicos e comerciais relevantes.

O serviço de Internet não pode ser usado para transmitir, recuperar ou armazenar quaisquer comunicações de natureza discriminatória ou de assédio ou que sejam depreciativas para qualquer indivíduo ou grupo, obsceno ou pornográfico, ou de natureza difamatória ou ameaçadora por “correntes” ou qualquer outra finalidade que é ilegal ou para ganho pessoal.

6.3 CLASSIFICAÇÃO DO USUÁRIO

Todos os usuários devem ter conhecimento dessas políticas de segurança e devem informar violações ao Administrador de Segurança. Além disso, todos os usuários devem estar em conformidade com a Política de uso aceitável definida neste documento. A empresa estabeleceu os seguintes grupos de usuários e definiu os privilégios e responsabilidades de acesso:

Categoria do usuário	Privilégios e Responsabilidades
Usuários do Departamento (Funcionários)	Acesso à aplicativos e bancos de dados, conforme necessário para a função de trabalho (VERMELHO E /ou VERDE apurado).
Administradores de Sistema	Acesso a sistemas de computadores, roteadores, hubs e outras tecnologias de infraestrutura necessárias para o trabalho. Acesso a informações confidenciais apenas com base em "necessidade de saber".
Administrador de Segurança	Maior nível de segurança. Acesso permitido a todos os sistemas de computadores, bancos de dados, firewalls e dispositivos de rede, conforme necessário para a função de trabalho.
Analistas de TI /Programador	Acesso à aplicativos e bancos de dados conforme necessário para uma função de trabalho específica. Não autorizado a acessar roteadores, firewalls ou outros dispositivos de rede.
Contratados/Consultores	Acesso à aplicativos e bancos de dados, conforme necessário para funções de trabalho específicas. Acesso a roteadores e firewall somente se necessário para a função job.

	Conhecimento de políticas de segurança. O acesso à informações e sistemas da empresa deve ser aprovado por escrito pelo diretor / CEO da empresa.
Outras agências e parceiros de negócios	Acesso à aplicativos e bancos de dados, conforme necessário para funções de trabalho específicas. Acesso a roteadores e firewall somente se necessário para a função job. Conhecimento de políticas de segurança. O acesso à informações e sistemas da empresa deve ser aprovado por escrito pelo diretor / CEO da empresa.
Público Geral	O acesso é limitado à aplicativos executados em servidores da Web públicos. O público em geral não terá permissão para acessar informações confidenciais.

6.4 Monitoramento do Uso de Sistemas de Computação

A empresa tem o direito e a capacidade de monitorar informações eletrônicas criadas e / ou comunicadas por pessoas que usam sistemas e redes de computadores da empresa, incluindo mensagens de e-mail e uso da Internet. Não é política ou intenção da empresa monitorar continuamente todo o uso do computador por funcionários ou outros usuários dos sistemas de computadores e da rede da empresa. No entanto, os usuários dos sistemas devem estar cientes de que a empresa pode monitorar o uso, incluindo, mas não limitado a padrões de uso da Internet (por exemplo, acesso ao site, duração on-line, horário de acesso) e arquivos eletrônicos dos funcionários e mensagens na medida necessária para assegurar que à Internet e outras comunicações eletrônicas estejam sendo usadas em conformidade com a lei e com a política da empresa.

7 Controle de Acesso

Um componente fundamental da nossa política de segurança cibernética é o controle do acesso aos recursos de informações críticas que exigem proteção contra divulgação ou modificação não autorizada. O significado fundamental do controle de acesso é que as permissões são atribuídas a indivíduos ou sistemas que estão autorizados a acessar recursos específicos. Controles de acesso existem em várias camadas do sistema, incluindo a rede. O controle de acesso é implementado pelo ID de logon e pela senha. No nível do aplicativo e do banco de dados, outros métodos de controle de acesso podem ser implementados para restringir ainda mais o acesso. O aplicativo e os sistemas de banco de dados podem limitar o número de aplicativos e bancos de dados disponíveis para os usuários com base em seus requisitos de trabalho.

7.1 Sistemas de usuários e Acesso à Rede – Identificação Normal do Usuário

Todos os usuários deverão ter um ID de logon e senha exclusivos para acesso aos sistemas. A senha do usuário deve ser mantida em sigilo e NÃO DEVE ser compartilhada com o pessoal de gerenciamento e supervisão e / ou com qualquer outro funcionário. Todos os usuários devem cumprir as seguintes regras referentes à criação e manutenção de senhas:

- ✓ A senha não deve ser encontrada em nenhum dicionário em inglês ou no estrangeiro. Ou seja, não use nenhum nome, substantivo, verbo, advérbio ou adjetivo comum. Estes podem ser facilmente quebrados usando “ferramentas de hackers” padrão.
- ✓ As senhas não devem ser postadas em terminais de computador ou perto dele ou de outra forma estar prontamente acessíveis na área do terminal.
- ✓ A senha deve ser alterada a cada (100 dias).
- ✓ As contas de usuários serão congeladas após 5 tentativas de login sem sucesso.
- ✓ IDs e senhas de logon serão suspensos após (30 dias) desuso.

Os usuários não têm permissão para acessar arquivos de senha em nenhum componente da infraestrutura de rede. Os arquivos de senhas nos servidores serão monitorados para acesso por usuários não autorizados. Copiar, ler, excluir ou modificar um arquivo de senha em qualquer sistema de computador é proibido.

Os usuários não poderão fazer logon como administrador do sistema. Os usuários que precisam desse nível de acesso aos sistemas de produção devem solicitar uma conta de acesso especial, conforme descrito em outras partes deste documento.

Os IDs e senhas de logon dos funcionários serão desativados assim que possível, se o funcionário for demitido, demitido, suspenso, demitido ou deixar o emprego do escritório da empresa.

Os supervisores / gerentes devem entrar em contato direto e imediato com o gerente de TI da empresa para relatar a mudança no status do funcionário que exija o cancelamento ou a modificação dos privilégios de acesso de logon do funcionário.

Os funcionários que esquecerem sua senha devem ligar para o departamento de TI para obter uma nova senha atribuída a sua conta. O funcionário deve identificar-se pela matrícula para o departamento de TI.

Os funcionários serão responsáveis por todas as transações que ocorrem durante as sessões de Logon iniciadas pelo uso da senha e do ID do funcionário. Os funcionários não devem fazer logon em um computador e permitir que outro indivíduo use o computador ou compartilhe o acesso aos sistemas do computador.

7.2 Acesso do Administrador do Sistema

Administradores de sistema, administradores de rede e administradores de segurança terão acesso (tipo de acesso) a sistemas host, roteadores, hubs e firewalls, conforme necessário para cumprir as obrigações de seu trabalho.

Todas as senhas do administrador do sistema serão EXCLUÍDAS imediatamente depois que qualquer funcionário que tenha acesso as senhas for demitido ou, de outra forma, deixar o emprego da empresa.

Apenas o administrador de sistemas e o CIO estão autorizados a entrar na sala de servidores, a não ser em caso excepcional, seja pelo não comparecimento do administrador de sistemas e do CIO na instituição, poderá ser feito por outro profissional da área de TI lotado na Coordenadoria de Informática. Nos casos de manutenção de equipamentos dentro da sala de servidores, profissionais externos poderão acessar, desde que acompanhados por pessoal autorizado.

7.3 Acesso Especial

Contas de acesso especiais são fornecidas a indivíduos que exigem privilégios temporários de administrador do sistema para executar seu trabalho. Essas contas são monitoradas pela empresa e exigem a permissão do gerente de TI da empresa do usuário. O monitoramento das contas especiais de acesso é feito inserindo os usuários em uma área específica e periodicamente gerando relatórios para o gerenciamento. Os relatórios mostrarão quem tem atualmente uma conta de acesso especial, por que motivo e quando expirará. As contas especiais expiram em (X # de) dias e não serão automaticamente renovadas sem permissão por escrito.

7.4 Conectando-se a redes de terceiros

Essa política é estabelecida para garantir um método seguro de conectividade fornecido entre a empresa e todas as empresas de terceiros e outras entidades necessárias para trocar informações eletronicamente com a empresa.

“Terceiros” refere-se a fornecedores, consultores e parceiros de negócios que fazem negócios com a empresa e outros parceiros que precisam trocar informações com a empresa. Conexões de rede de terceiros devem ser usadas somente pelos funcionários de terceiros, apenas para fins comerciais da empresa. A empresa terceirizada garantirá que somente usuários autorizados terão permissão para acessar informações na rede da empresa. O terceiro não permitirá que o tráfego da Internet ou outro tráfego de rede privada flua para a rede. Uma conexão de rede de terceiros é definida como uma das seguintes opções de conectividade:

- ✓ Uma conexão de rede terminará em um (a ser especificado) e o terceiro estará sujeito às regras padrão de autenticação da empresa.

Esta política se aplica a todas as solicitações de conexão de terceiros e a quaisquer conexões de terceiros existentes. Nos casos em que as conexões de rede de terceiros existentes não atenderem aos requisitos descritos neste documento, elas serão reprojetadas conforme necessário.

Todas as solicitações de conexões de terceiros devem ser feitas enviando uma solicitação por escrito e sendo aprovadas pela empresa.

7.5 Conectando Dispositivos à Rede

Somente dispositivos autorizados podem estar conectados à (s) rede (s) da empresa. Dispositivos autorizados incluem PCs e estações de trabalho de propriedade da empresa que cumprem as

diretrizes de configuração da empresa. Outros dispositivos autorizados incluem dispositivos de infraestrutura de rede usados para gerenciamento e monitoramento de rede.

Os usuários não devem se conectar à rede: computadores que não sejam da empresa e que não sejam autorizados, de propriedade e / ou controlados pela empresa. Os usuários são especificamente proibidos de especificar à rede da empresa.

OBSERVAÇÃO: os usuários não estão autorizados a conectar qualquer dispositivo que altere as características de topologia da rede ou de dispositivos de armazenamento não autorizados, por exemplo, pen drives e CDs graváveis.

7.6 Acesso Remoto

Somente pessoas autorizadas podem acessar remotamente a rede da empresa. O acesso remoto é fornecido aos funcionários, contratados e parceiros de negócios da empresa que têm uma necessidade comercial legítima de trocar informações, copiar arquivos ou programas ou acessar aplicativos de computador. A conexão autorizada pode ser um PC remoto para a rede ou uma rede remota para a conexão de rede da empresa. O único método aceitável de se conectar remotamente à rede interna é usar um ID seguro.

7.7 Acesso Remoto Não Autorizado

A ligação de (por exemplo, hubs) a um PC ou estação de trabalho de um usuário que esteja conectado à LAN da empresa não é permitida sem a permissão por escrito da empresa. Além disso, os usuários não podem instalar software pessoal projetado para fornecer controle remoto do PC ou da estação de trabalho. Esse tipo de acesso remoto ignora os métodos altamente seguros autorizados de acesso remoto e representa uma ameaça à segurança de toda a rede.

8 Penalidade por Violação de Segurança

A empresa leva a questão da segurança a sério. As pessoas que usam os recursos de tecnologia e informação da empresa devem estar cientes de que podem ser disciplinadas se violarem essa política. Em caso de violação desta política, um funcionário da empresa pode estar sujeito a medidas disciplinares. A disciplina específica imposta será determinada caso a caso, levando em consideração a natureza e a gravidade da violação da Política de Segurança Cibernética, violações anteriores da política cometida pelas leis individuais, estaduais e federais e todas as outras leis

relevantes em formação. A disciplina que pode ser tomada contra um funcionário deve ser administrada de acordo com as regras ou políticas apropriadas e com o Manual de Normas da empresa.

Em um caso em que o acusado não é um funcionário da empresa, o assunto deve ser submetido ao CIO. O CIO pode encaminhar as informações para que o RH a fim de efetuar a aplicação da lei e / ou para representação de acusações criminais contra o (s) alegado (s) infrator (es).

9 Procedimentos de Manuseio de Incidentes de Segurança

Esta seção fornece algumas diretrizes e procedimentos de políticas para lidar com incidentes de segurança. O termo “incidente de segurança” é definido como qualquer evento irregular ou adverso que ameace a segurança, integridade ou disponibilidade dos recursos de informação em qualquer parte da rede da empresa. Alguns exemplos de incidentes de segurança são:

- ✓ Acesso ilegal de um sistema de computador da empresa. Por exemplo, um hacker faz logon em um servidor de produção e copia o arquivo de senha.
- ✓ Danos ao sistema de computador ou rede da empresa causados por acesso ilegal. Liberar um vírus ou worm seria um exemplo.
- ✓ Ataque de negação de serviço contra um servidor da web da empresa. Por exemplo, um hacker inicia uma enxurrada de pacotes contra um servidor da Web projetado para causar falhas no sistema.
- ✓ Uso malicioso de recursos do sistema para iniciar um ataque contra outro computador fora da rede da empresa. Por exemplo, o administrador do sistema percebe uma conexão com uma rede desconhecida e um processo estranho acumulando muito tempo do servidor.

Os funcionários, que acreditam que seus sistemas de terminal ou computador tenham sido submetidos à um incidente de segurança, ou que tenham sido acessados ou usados de maneira inadequada, devem comunicar a situação imediatamente ao (seu representante). O funcionário não deve desligar o computador ou excluir arquivos suspeitos. Deixar o computador à condição em que estava quando o incidente de segurança foi descoberto ajudará a identificar à origem do problema e a determinar as etapas que devem ser tomadas para solucionar o problema.

10 Das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes.

Conforme a resolução (nº 4.893/2021 e 4.658/2018) a Agencia de Fomento deve comunicar tempestivamente ao Banco Central do Brasil sobre as ocorrências de incidentes relevantes e das interrupções relevantes.

Registrar e analisar a causa e impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição.

Algumas ações recomendadas exigirão da Diretoria da AGÊNCIA DE FOMENTO decisão de investimento, visando atingir com as soluções propostas níveis acima do objetivo mínimo aceitável de continuidade de negócios, o que se traduz em melhoria significativa de eficácia de recuperação.

Conforme PCCN, relativamente à decisão de entrada em situação de contingência, recomendam-se os seguintes níveis de alçada:

Incidente	Tomadores de Decisão
Falha em Ativo de TI	Coordenador de TI + Presidente ou 1 Diretor

Na sequência são apresentados os planos de ação, divididos por ativo da empresa com risco de falhas de impacto global:

Ativo: Rede de Dados Interna (LAN)

AMEAÇAS	VULNERABILIDADE	RISCOS	
Falha no equipamento (switch)	Fornecimento de acesso à rede de forma interrompida, por inexistência de redundância.	Parada da rede corporativa - LAN	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados interna (LAN)	Coordenador de TI	Interrupção não tolerável	Implantar ação imediatamente
Viabilizar a disponibilização da rede em modo redundante.	Coordenador de TI, Diretoria Executiva e Conselho Deliberativo		Implantar ação a médio prazo

Agência de FOMENTO do Estado do Tocantins

Ativo: Link de dados (WAN) – Internet

AMEAÇAS	VULNERABILIDADE	RISCOS	
Interrupção do serviço de fornecimento de acesso internet (WAN) pelo prestador do serviço e falha no equipamento (modem/roteador).	Fornecimento de acesso à internet de forma interrompida por inexistência de redundância.	Perda de acesso à internet com indisponibilidade dos serviços de e-mail, WEB e com possibilidade de perdas de transações eletrônicas.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados WAN.	Coordenador de TI	Interrupção não tolerável	Implantar ações imediatamente
Viabilizar o fornecimento de acesso em modo redundante para disponibilizar o acesso a internet e seus serviços de forma ininterrupta.	Coordenador de TI, Diretoria Executiva e Conselho Deliberativo		

Agência de FOMENTO do Estado do Tocantins

Ativo: Intranet

AMEAÇA	VULNERABILIDADE	RISCO	
Interrupção do serviço de Intranet, falha no servidor responsável por suportar o serviço intranet.	Fornecimento de acesso ao serviço intranet interrompida.	Perda de acesso aos serviços disponibilizados na intranet.	

AÇÕE	RESPONSÁVEIS	PRAZO MÁXIMO -	PRIORIDADE
Efetuar procedimento corretivo utilizando-se de backup para restauração mais relevante do ambiente intranet	Coordenador de TI	24 horas	Implantar ação a médio prazo

Ativo: Link de Voz (telefonia)

AMEAÇA	VULNERABILIDADE	RISCO	
Interrupção do serviço de voz.	Fornecimento de link de voz interrompido por falha adversa, sem aviso prévio e por inexistência de	Perder a comunicação via telefone com as entidades externas à (Agência De Fomento, participantes, beneficiários	

AÇÕE	RESPONSÁVEIS	PRAZO MÁXIMO -	PRIORIDADE
Utilizar de forma emergencial os telefones celulares corporativos.	Colaboradores portadores desse recurso	Interrupção não tolerável	Implantar ações imediatamente
Viabilizar o fornecimento de link de voz em modo redundante, para disponibilizar este serviço de forma ininterrupta.	Coordenador de Administração e Diretoria Executiva		
Informar a interrupção e a previsão de retorno à Agencia de Fomento.	Assessoria de Comunicação		

Agência de FOMENTO do Estado do Tocantins

Ativo: Servidor de Banco de Dados

AMEAÇAS	VULNERABILIDADE	RISCOS	
Falha no equipamento (servidor).	Interrupção do acesso às informações core da empresa.	Parada do servidor.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer a funcionalidade física do servidor (Componentes eletrônicos)	Coordenador de Ti	Interrupção não tolerável	Implantar ações imediatamente
Reestabelecer a funcionalidade do banco de dados do servidor (Base de dados)	Coordenador de Ti		
Viabilizar provisionamento para substituição do equipamento em caso de falha e/ou criação de ambiente redundante com sincronização dos dados.	Coordenador de TI e Diretoria Executiva		Implantar ação a médio prazo

Ativo: Sistema Integrado de Gestão

AMEAÇA	VULNERABILIDADE	RISCO	
Falha do sistema; Descontinuidade na prestação de serviço do fornecedor do sistema	Impacto nos processos que utilizam o sistema.	Atualização de versão com falha.	

AÇÕE	RESPONSÁVEIS	PRAZO MÁXIMO -	PRIORIDADE
Reestabelecer o sistema de forma funcional.	Coordenador de Ti	Interrupção não tolerável	Implantar ações imediatamente
Viabilizar provisionamento para melhoria / atualização do sistema	Coordenador de TI e Diretoria Executiva		
Elaborar estudo de viabilidade para substituição do fornecedor			Implantar ação a médio

Ativo: Site Internet da FOMENTO

AMEAÇA	VULNERABILIDADE	RISCO	
Falha na prestação do serviço do provedor Internet; Falha no link de dados.	Impacto nos processos e clientes que utilizam os serviços	Indisponibilidade dos serviços prestados aos clientes.	

AÇÕE	RESPONSÁVEIS	PRAZO MÁXIMO -	PRIORIDADE
Reestabelecer a disponibilização do site de forma emergencial.	Coordenador de Ti	24 horas	Implantar ações imediatamente
Informar a interrupção e a previsão de retorno à Agência de Fomento.	Assessoria de Comunicação		
Viabilizar criação de redundância dos serviços indispensáveis aos clientes e disponibilizados na internet	Coordenador de TI e Diretoria Executiva		Implantar ação a médio prazo

11 Da Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem.

A Agencia de Fomento utilizará a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem mediante prévia autorização do da Diretoria, na forma de regulamentação específica, Resolução N.º 4.658/2018 e 4.752/2019, observando, ainda, procedimentos que contemplem:

I. A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;

II. A verificação (de forma documentada) da capacidade do potencial prestador de serviço de assegurar:

a) O cumprimento da legislação e da regulamentação em vigor;

b) O acesso da Agencia de Fomento aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço;

d) A sua aderência a certificações exigidas pela Agencia de Fomento para a prestação do serviço a ser contratado;

e) O acesso da Agencia de Fomento aos relatórios elaborados por empresa de auditoria especializada independente contratada para o fim específico, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) A identificação e a segregação dos dados dos clientes da Agencia de Fomento por meio de controles físicos ou lógicos;

h) A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da Agencia de Fomento.

Na avaliação da relevância do serviço a ser contratado a Agencia de Fomento considerará a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

Mitigação dos efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos usados por meio de internet.

O contratado deverá disponibilizar a Agencia de Fomento, ao menos um dos seguintes serviços:

I – Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Agencia de Fomento implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela Agencia de Fomento ou por ela adquiridos;

II – Implantação ou execução de aplicativos desenvolvidos pela Agencia de Fomento, ou por ela adquirido, utilizando recursos computacionais disponibilizados pelo prestador de serviço;

III – execução, por meio de internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais disponibilizados pelo prestador de serviços.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, serão comunicados ao Banco Central do Brasil, contendo as seguintes informações:

I – A denominação da empresa contratada até 10 (dez) dias após a contratação do serviço;

II – Os serviços relevantes a serem contratados.

Parágrafo único: as alterações contratuais que impliquem em modificação das informações acima, devem ser comunicadas ao Banco Central do Brasil até 10 dias após a alteração contratual.

Em caso de interrupção dos serviços de processamento e armazenamento de dados e de computação em nuvem, abrangendo os cenários que considerem a substituição da empresa contratada, a Agencia de Fomento deve proceder conforme REGULAMENTO

DE LICITAÇÕES E CONTRATOS DA AGENCIA DE FOMENTNO e em conformidade com a lei nº 13.303, de 30/6/2016.

12 Responsável pela estrutura de Gerenciamento da Política Cibernética e demais atos.

Ficará responsável pela estrutura de gerenciamento da Política de Segurança Cibernética o Coordenador de Tecnologia de Informação da Agencia de Fomento, de Fomento, devendo o referido setor de TI, Implantar a referida politica nos termos expostos, informar qualquer situação de perigo a Diretoria Executiva, fiscalizar, efetuar testes periódicos de segurança e emitir relatórios semestrais.

13 DISPOSIÇÕES FINAIS

Este documento visa formalizar as políticas e estratégias para a Estrutura de Gerenciamento da Política de Segurança Cibernética da Agência de Fomento do Estado do Tocantins, em atendimento à Resolução nº 4.658, de 26 de abril de 2018 do Banco Central do Brasil e normativos vigentes.

A Política em questão deverá ser revisada no mínimo anualmente e, caso tenham alterações ou novas implementações, será encaminhada para aprovação da Diretoria Executiva e ao Conselho de Administração, para deliberação final.

Esta Política de Segurança Cibernética entra em vigor na data de sua publicação.

TIAGO DE ALMEIDA TORRES
Coordenador de Tecnologia