Diário Oficial
Municípios de Santa Catarina

Sexta-feira, 22 de dezembro de 2023 às 15:43, Florianópolis - SC

PUBLICAÇÃO

Nº 5459516: RESOLUÇÃO Nº 248/2023

ENTIDADE

CINCATARINA - Consórcio Interfederativo Santa Catarina

https://www.diariomunicipal.sc.gov.br/?q=id:5459516

Resolução n. 0248/2023

TORNA PÚBLICO O PLANO DE AÇÃO DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PASTIC) DO CONSÓRCIO INTERFEDERATIVO SANTA CATARINA – CINCATARINA.

O Presidente do **Consórcio Interfederativo Santa Catarina - CINCATARINA,** Sr. **Wilson Ribeiro Cardoso Junior,** Prefeito Municipal de Fraiburgo - SC, no uso de suas atribuições legais, contidas no Protocolo de Intenções e Contrato de Consórcio Público;

CONSIDERANDO a Resolução n. 0240/2023 de 18 de dezembro de 2023, que tornou pública a Identidade Estratégica do CINCATARINA.

CONSIDERANDO a Resolução n. 0246/2023 de 22 de dezembro de 2023, que tornou pública a Cadeia de Valor e o Plano Estratégico do CINCATARINA apresentando os objetivos de atuação do Consórcio Público, em alinhamento com a Identidade Estratégica.

RESOLVE:

Art. 1º Tornar público o Plano de Ação de Segurança em Tecnologia da Informação e Comunicação (PASTIC), nos termos do Anexo Único parte integrante da presente resolução, para produzir seus efeitos legais.

Art. 2º Esta resolução entra a vigor na data de sua publicação, revogadas as disposições em contrário.

Florianópolis SC, 22 de dezembro de 2023.

Wilson Ribeiro Cardoso Junior
Prefeito de Fraiburgo
Presidente do CINCATARINA

Documento original eletrônico assinado digitalmente nos termos do Artigo 10 da Medida Provisória nº 2.200-2/2001 e Lei Federal nº 14.063/2020

ANEXO ÚNICO

PLANO DE AÇÃO DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PASTIC)

A segurança da informação e comunicação envolve múltiplos aspectos da Entidade. Desde o controle dos acessos físicos às suas dependências; acessos lógicos a infraestrutura de dados; políticas de uso dos recursos de tecnologia até os locais de armazenamento de informações. Também abrange processos de trabalhos, relações com municípios consorciados, fornecedores ou prestadores de serviço e o uso adequado das ferramentas e serviços da tecnologia da informação, transparência, zelo pela imagem da Entidade e publicação de normativas.

Nesse sentido, o Plano de Ação de Segurança da Tecnologia da Informação e Comunicação (PASTIC) do Consórcio Interfederativo Santa Catarina – CINCATARINA estabelece diretrizes e critérios suficientes à implementação de técnicas e recursos de segurança para os ativos de tecnologia da informação e comunicação, reconhecidos como valiosos e fundamentais para que a Entidade desempenhe suas atividades.

Trata-se do planejamento e definição de ações necessárias para a promoção e o fortalecimento da Segurança da Informação e Comunicação do CINCATARINA, nos termos estabelecidos pela sua identidade estratégica, cadeia de valores e o planejamento estratégico, promovendo ações e a adoção de mecanismos voltados à sua segurança.

As medidas para a implantação do PASTIC, sua manutenção e melhorias estão em total conformidade com a Lei Geral de Proteção de Dados (LGPD), bem como com as recomendações estabelecidas nas normas e boas práticas nacionais e internacionais. Também está regulamentado e monitorado com base na avaliação do mapa de riscos, suas ações preventivas e de contingências. Estes riscos devem ser tratados como ações que comprometem a continuidade dos trabalhos da Entidade, afetando não só todo o fluxo das atividades desempenhadas, mas também as que também podem gerar danos à sua imagem.

Vê-se, então, que o mapeamento de riscos tem como objetivo prever os possíveis riscos envolvidos nos processos de estratégias de atuação do Consórcio Público, buscando

CNPJ: 12.075.748/0001-32
www.cincatarina.sc.gov.br
cincatarina@cincatarina.sc.gov.br
Sede do CINCATARINA
Rua General Liberato Bittencourt, 1885, 13º Andar, Sala 1305, Bairro Canto
Florianópolis/Estado de Santa Catarina – CEP 88.070-800
Telefone: (48) 3380 1620
Central Executiva do CINCATARINA
Rua Nereu Ramos, 650, 1º Andar, Sala 102, Centro
Fraiburgo/Estado de Santa Catarina – CEP 89.580-000
Telefone: (48) 3380 1621

antever dificuldades diversas enfrentadas e instituir políticas para garantir a segurança, proteção e a disponibilidade das informações através do apontamento: dos riscos considerados de maior criticidade para o andamento das atividades, dos danos que estes riscos podem gerar para a Entidade caso aconteça, das ações preventivas para evitar ou mitigar esses riscos e as ações de contingências.

Em atendimento ao **OBJETIVO 34** do Plano Estratégico do CINCATARINA para promover a implementação e manutenção do PASTIC, são os **OBJETIVOS ESPECÍFICOS** e suas **Ações Estratégicas:**

OBJETIVO ESPECÍFICO 1 – Prevenir indisponibilidade de Energia Elétrica pela concessionária.

Ações Estratégicas:

- Utilizar equipamentos do tipo Fonte de Alimentação Ininterrupta – Nobreak, podendo ser equipamentos individuais, mas preferencialmente de uma rede de energia exclusiva para o setor de tecnologia da informação conectada à um nobreak de grande porte e com autonomia para suportar as necessidades dos trabalhos essenciais.
- Utilizar sistema de monitoramento de energia elétrica visando o envio de alertas sobre a ocorrência de uma eventual falta de energia na fonte primária.
- Possuir *Backup* de equipamentos da infraestrutura para eventuais substituições visando o rápido reestabelecimento dos serviços aos sistemas de informática, especialmente em casos de defeitos causados por oscilações de energia.

OBJETIVO ESPECÍFICO 2 – Prevenir Indisponibilidade de Link de Internet

Ações Estratégicas:

- Contratar empresa certificada e homologada pela ANATEL (Agência Nacional de Telecomunicações) para o fornecimento do link de internet. Esta certificação garante que a empresa atendeu aos requisitos exigidos pela agência reguladora para a prestação de serviços relacionadas a telecomunicações.

CNPJ: 12.075.748/0001-32
www.cincatarina.sc.gov.br
cincatarina@cincatarina.sc.gov.br

Sede do CINCATARINA
Rua General Liberato Bittencourt, 1885, 13º Andar, Sala 1305, Bairro Canto
Florianópolis/Estado de Santa Catarina – CEP 88.070-800
Telefone: (48) 3380 1620

Central Executiva do CINCATARINA
Rua Nereu Ramos, 650, 1º Andar, Sala 102, Centro
Fraiburgo/Estado de Santa Catarina – CEP 89.580-000
Telefone: (48) 3380 1621

- Possuir cláusula contratual com a contratada para o cumprimento da SLA (*Service Level Agreement* - Acordo de Nível de Serviço) para eventuais resoluções de problemas. Estas são medidas previstas em contrato para que, em determinados casos, a prestadora esteja obrigada a atender e a solucionar uma eventual indisponibilidade dos serviços em um intervalo de tempo o qual foi previamente acordado.
- Contratar link de internet para backup de uma empresa "B" onde o requisito seja de possuir rotas diferentes de transmissão de dados quando compactado com a empresa "A". Busca-se, dessa forma, uma rota alternativa à transmissão de dados, medida como prevenção no caso de uma eventual falha na rede causada por eventos como rompimentos de cabos em vias públicas ou até mesmo por eventos climáticos.
- Em caso de queda do link principal, acionar link de *backup* de internet. Ajustar as devidas configurações para que este passe a atuar como link principal fazendo com que a queda do link primário seja imperceptível para os usuários ou sistemas ou que cause o menor *downtime* possível.

OBJETIVO ESPECÍFICO 3 – Prevenir falhas na camada de enlace de dados ou camada física de rede associadas à instabilidade ou parada de dispositivos ou serviços relacionados à rede de computadores como *gateway*, *switch*, roteadores ou demais equipamentos da camada de transporte.

Ações Estratégicas:

- Realizar manutenção preventiva nos ativos de rede, uma vez que é fundamental manter e acompanhar a saúde dos equipamentos de infraestrutura, identificando possíveis falhas físicas e prevendo eventos como o superaquecimento das instalações ou outros problemas que possam vir a acontecer.
- Manter equipamentos de *backup* para eventuais substituições em caso de falhas nos equipamentos principais. Ativos de rede possuem um regime de carga de trabalho categorizados como de uso severo. Regimes de trabalho de

CNPJ: 12.075.748/0001-32
www.cincatarina.sc.gov.br
cincatarina@cincatarina.sc.gov.br
Sede do CINCATARINA
Rua General Liberato Bittencourt, 1885, 13º Andar, Sala 1305, Bairro Canto
Florianópolis/Estado de Santa Catarina – CEP 88.070-800
Telefone: (48) 3380 1620
Central Executiva do CINCATARINA
Rua Nereu Ramos, 650, 1º Andar, Sala 102, Centro
Fraiburgo/Estado de Santa Catarina – CEP 89.580-000
Telefone: (48) 3380 1621

24/7 (vinte e quatro por sete), ou seja, 24 (vinte e quatro) horas por dia durante os 7 (sete) dias na semana.

- Em caso de falhas, proceder com a adequação das rotas para equipamentos paralelos e, nos casos mais graves, seguir com a substituição do equipamento que apresentou falha por outro de *backup* para assegurar o reestabelecimento dos serviços e a continuidade dos trabalhos.

OBJETIVO ESPECÍFICO 4 – Prevenir falha humana e ataques cibernéticos. A falha humana não diz respeito somente ao erro operacional do usuário, mas também à gestão da infraestrutura da tecnologia da informação como a falta de políticas de atualizações dos sistemas operacionais ou adoção de mecanismos de defesas. Importante destacar que, em sua grande maioria, os ataques virtuais, mesmo com o objetivo de atingir ao servidor de arquivos ou do sistema, não são diretamente voltados a estes servidores, pois para fazê-lo uma série de camadas de segurança devem ser superadas e, por isso, esses ataques ocorrem buscando o elo mais fraco: as estações de trabalho e a falha humana.

Ações Estratégicas:

- Promover treinamentos específicos sobre segurança digital para todos os empregados públicos visando o conhecimento e aplicabilidade das principais técnicas usadas por cibercriminosos, como agem e algumas das ameaças como *Worms, Trojans, Spyware, Malware, Phishing, Spam* entre outras, bem como a adoção de políticas internas sobre o uso de equipamentos e recursos de tecnologia da informação.
- Utilizar sistemas de defesas como *Firewall,* Antivírus, AntiSpam, checagem de DNS reverso, controle de e-mails, políticas de controle de acesso nas estações de trabalho. Realizar o monitoramento nos links de internet a fim de identificar eventuais tráfegos de dados fora das rotinas de trabalho que indiquem potenciais ataques.
- Realizar manutenção periódica adotando rotinas preventivas com o monitoramento de *logs* de eventos, atualizações de vulnerabilidades de segurança nos sistemas operacionais e *softwares* e atualizações para todos os *patchs* de segurança devidamente implantados. Utilização somente de

softwares genuínos e registrados sem qualquer tipo de *crack* ou artifícios para ativação de softwares.

- Utilizar senhas fortes e com duplo fator de autenticação. Sistemas automatizados para o bloqueio de acesso após números de tentativas de acesso inválidos ou fora da geolocalização definida para o uso. Política de conscientização sobre a guarda e armazenamento de senhas.
- Padronização de sistemas e métodos nas integrações ou eventuais desligamentos dos empregados públicos, garantindo o acesso somente enquanto houver o vínculo com a Entidade assim como políticas de uso de recursos de tecnologia bem definidas.
- Implementar políticas de solicitações de acesso feitas somente pelo gestor do setor, assim como a atenção dos gestores quanto a remoção dos acessos quando for o caso de realocação para outro setor.
- Implementar políticas de bloqueio na camada de perímetro. Nesta camada ocorrem os tráfegos de troca de pacotes entre o ambiente interno e externo. Então, endereços e países de origem duvidosa que a Entidade não se relaciona devem ser bloqueados deixando o tráfego restrito para conteúdos validados.
- Utilizar redes virtuais isoladas com políticas de acesso bem definidas e protegidas do restante da infraestrutura como redes de telefonia, *wi-fi*, circuito de videomonitoramento, acesso remoto entre outras.
- Executar programas e rotinas de cópias de segurança (*backup*) bem definidas, com o armazenamento dos arquivos em ambiente fora das instalações do CINCATARINA para garantir que, mesmo em caso de falhas físicas dos servidores, ataques virtuais ou até mesmo em casos de roubos, as informações possam ser recuperadas.
- Atentar ao sinal de alerta ou quando identificada uma eventual atividade suspeita. Havendo a necessidade deverá ocorrer o bloqueio da estação de trabalho ou dispositivo potencialmente inseguro. Este processo deverá ser seguido da revogação dos acessos da estação ou dispositivo afetado e do bloqueio das credenciais de acesso do usuário responsável pelo dispositivo.

Caso alguma ação comprometa a infraestrutura de dados, recorrer a restauração dos arquivos contidos em backup.

OBJETIVO ESPECÍFICO 5 – Prevenir acesso físico não autorizado.

Ações Estratégicas:

- Implementar políticas de controle de acesso (empregados públicos ou pessoal autorizado e visitantes, entregadores ou prestadores de serviços).
- Utilizar dispositivos de controle de acesso com senhas, crachás ou reconhecimento facial que permitam o acesso somente ao pessoal autorizado.
- Utilizar sistemas de segurança eletrônica como central de alarmes ou circuito de videomonitoramento.
- Caso ocorra a invasão ou acesso indevido no perímetro, acionar as autoridades responsáveis.

OBJETIVO ESPECÍFICO 6 – Insegurança jurídica para o CINCATARINA movida por pessoas más intencionadas sobre o monitoramento de relatórios de acessos aos repositórios de arquivos, serviços de telefonia, circuito de videomonitoramento, e-mails, controladores de acesso etc.

Ações Estratégicas:

- Elaborar documentos internos como termos de ciência de uso dos recursos da tecnologia da informação e comunicação destacando políticas de uso da rede sem fio, rede de dados, telefonia, e-mail corporativo etc.
- Implementar termos de ciência sobre o uso de controladores de acessos, circuito de videomonitoramento, bem como o eventual monitoramento das atividades digitais quando indicar possível ameaça cibernética ou fatos que tornem a ação necessária.
- Instituir formas de responsabilização por má conduta ou violações aos termos assumidos durante o uso dos recursos de tecnologia da informação.

CNPJ: 12.075.748/0001-32
www.cincatarina.sc.gov.br
cincatarina@cincatarina.sc.gov.br

Sede do CINCATARINA
Rua General Liberato Bittencourt, 1885, 13º Andar, Sala 1305, Bairro Canto
Florianópolis/Estado de Santa Catarina – CEP 88.070-800
Telefone: (48) 3380 1620

Central Executiva do CINCATARINA
Rua Nereu Ramos, 650, 1º Andar, Sala 102, Centro
Fraiburgo/Estado de Santa Catarina – CEP 89.580-000
Telefone: (48) 3380 1621

Considerando os benefícios decorrentes das **Ações Estratégicas** aqui propostas, a expectativa é de que o Plano de Ação em Segurança da Informação e Comunicação seja reconhecido com seu caráter estratégico para as atividades da Entidade.

Com a tomada das ações preventivas o resultado esperado deve ser a implantação de mecanismos que fortaleçam a segurança física e digital do CINCATARINA e dos recursos de tecnologia, mitigando eventos que possam gerar paradas não programadas e, dessa forma, diminuindo o tempo de inatividade (*downtime*).

Busca-se, portanto, segurança quanto à guarda e eventual recuperação de dados e informações nos casos de perda, seja por erro humano, ataques externos, catástrofes naturais ou outras ameaças; o zelo pelos ativos patrimoniais do CINCATARINA através de controles de acessos nas dependências da Entidade e a segurança jurídica com a implementação de termos de ciência sobre o uso de recursos de tecnologia de informação e comunicação.

Desta forma, o PLANO DE AÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO do CINCATARINA vem contribuir com a revisão metodológica e atualização nas políticas de comprometimento da Entidade em relação ao cumprimento da Lei Geral de Proteção de Dados (LGPD), programas de compliance e suas próprias diretrizes.

CNPJ: 12.075.748/0001-32
www.cincatarina.sc.gov.br
cincatarina@cincatarina.sc.gov.br

Sede do CINCATARINA
Rua General Liberato Bittencourt, 1885, 13º Andar, Sala 1305, Bairro Canto
Florianópolis/Estado de Santa Catarina – CEP 88.070-800
Telefone: (48) 3380 1620

Central Executiva do CINCATARINA
Rua Nereu Ramos, 650, 1º Andar, Sala 102, Centro
Fraiburgo/Estado de Santa Catarina – CEP 89.580-000
Telefone: (48) 3380 1621

Assinado digitalmente por:

WILSON RIBEIRO CARDOSO JUNIOR
•••.493.469-••
Data: 22/12/2023 15:22

e-Ciga

Ciga