jun/23

Guia de boas práticas em Segurança da Informação para Tribunais de Contas

Instituto Rui Barbosa
A Casa do Conhecimento dos Tribunais de Contas

Comitê de TI
Comitê de Tecnologia, Governança e Segurança da Informação dos TCs

TCESP
Tribunal de Contas
do Estado de São Paulo

PUBLICAÇÃO

Esta publicação é uma iniciativa do Comitê Técnico de Tecnologia, Governança e Segurança da Informação do Instituto Rui Barbosa

Comitê Técnico de Tecnologia, Governança e Segurança da Informação - IRB

Baixe a versão digital deste Guia.

ELABORAÇÃO
Fábio Correa Xavier - TCESP

DIAGRAMAÇÃO
Instituto Rui Barbosa - IRB

REVISÃO
José David de Araújo - TCESP
Ricardo Abade - TCESP

Conheça o Comitê Técnico de Tecnologia, Governança e Segurança da Informação do Instituto Rui Barbosa

EXPEDIENTE

Instituto Rui Barbosa
Gestão 2022-2023 - Diretoria

Presidente
Edilberto Pontes Lima

Vice-Presidentes
Cristiana de Castro Moraes
Vice-presidente desenvolvimento e políticas públicas

Inaldo da Paixão Santos Araújo
Vice-presidente de Auditoria

Ivan Lelis Bonilha
Vice-presidente de relações institucionais

Mário Manoel Coelho de Mello
Vice-presidente de desenvolvimento institucional

Sebastião Helvecio Ramos de Castro
Ensino, pesquisa e extensão

Suplentes da Vice-Presidência
Domingos Augusto Taufner
Felipe Galvão Puccioni
Lilian de Almeida Veloso Nunes Martins
Naluh Maria Lima Gouveia
Rosa Egídia Crispino Calheiro Lopes

Primeiro Secretário
Algir Lorenzon

Segundo Secretário
Fabrício Macedo Motta

Tesoureiro
Severiano José Costandrade de Aguiar

Conselho Fiscal
José Valdomiro Távora de Castro Júnior
Maria Elizabeth Cavalcante de Azevedo Picanço
Celmar Rech Luiz Eduardo Cherem
Carlos Thompson Costa Fernandes

Suplentes do Conselho Fiscal
Fernando Ribeiro Toledo
Estilac Martins Rodrigues Xavier
Cilene Lago Salomão
Inácio Magalhães Filho
Patrícia Lúcia Mendes Saboya

Equipe Técnica
Juraci Muniz Júnior
Coordenador Geral

Ana Perpétua Ellery Corrêa
Gerente de Políticas Públicas

Izabelli Lima
Gerente Supervisora

José Wesmey da Silva
Gerente Financeiro

Sandra Valéria de Morais Santos
Gerente Administrativa e Planejamento

Assessoria Técnica
Alisson Sousa Maciel
Fernanda Ferreira Aguiar
Geovana dos Santos Teixeira Ferreira
Iolanda Piancó Amorim
Lia Skaty Pinheiro

SUMÁRIO

Palavra Presidente do IRB

Conselheiro
Edilberto Ponte Lima

Anunciamos mais uma importante iniciativa do Instituto Rui Barbosa (IRB), por meio de seu Comitê de Tecnologia da Informação, dessa vez em prol da segurança digital do sistema de controle externo: o Guia de Boas Práticas em Segurança da Informação dos Tribunais de Contas.

Em um mundo em plena transformação digital, é de fundamental importância estarmos preparados para enfrentar os desafios que surgem. Por isso nossa preocupação em fornecer diretrizes claras e práticas para auxiliar na compreensão e implementação de medidas eficazes de segurança digital.

A segurança digital é uma responsabilidade compartilhada, cabendo a cada um contribuir para a proteção dos sistemas e dados. Por meio desse guia, visamos fortalecer as defesas contra ameaças cibernéticas, como ataques de hackers e furto de informações sensíveis, entre outros problemas.

Ao adotarmos as orientações presentes no guia, buscamos ampliar sensivelmente a segurança na integridade e na confidencialidade dos dados que utilizamos em nossas atividades, reforçando a confiança depositada nas instituições de controle externo.

Conhecimentos, boas práticas e experiências presentes no guia ajudam a promover um ambiente seguro e confiável para o desenvolvimento de nossas atividades.

Agradeço a todos os envolvidos nessa iniciativa, em especial aos integrantes do Comitê de Tecnologia da Informação do IRB, que tem realizado, sob a liderança do Conselheiro Carlos Neves, um trabalho profícuo.

Convido cada um a abraçar essa importante causa. Com uma estratégia bem definida e um plano de ação bem elaborado, seremos capazes de proteger nossos dados, sistemas e plataformas, ampliando a confiança depositada em nossas instituições.

Palavra

Presidente do TCESP

Conselheiro
Sidney Estanislau Beraldo

Impossível imaginar o mundo sem os avanços que a tecnologia tem nos proporcionado. Conceitos como governos digitais e inteligência artificial hoje são também imprescindíveis no setor público, que busca combinar a eficiência no uso dos recursos originários dos impostos pagos pelos cidadãos com a efetividade das políticas criadas para beneficiar a população.

Mas, se a pandemia nos mostrou claramente que podemos fazer quase tudo com a informática, deixou evidente o quão frágeis podem ser as ferramentas cibernéticas.

Para o Controle Externo, que trabalha com informações sigilosas e sensíveis das mais diversas administrações, segurança é fundamental. Nossa responsabilidade, como instituição, é proteger sistemas e dados, preservando a confiança de jurisdicionados e da sociedade. Daí a importância desta iniciativa, resultado da dedicação do Comitê de Tecnologia, Governança e Segurança da Informação do IRB.

Destacando a valiosa participação da equipe do Tribunal de Contas do Estado de São Paulo (TCESP) na elaboração deste manual, cumprimento os envolvidos pela clareza e objetividade, qualidades que certamente permitirão que nossos colaboradores adotem as melhores práticas em suas atividades cotidianas.

Agradecendo o empenho de todos os envolvidos, convido integrantes e servidores dos Tribunais de Contas brasileiros a conhecerem as medidas propostas neste documento. Juntos, poderemos enfrentar os desafios da modernidade com confiança e resiliência.

Palavra Presidente do Comitê

Conselheiro **Carlos Neves**

É com grande satisfação que apresentamos o Guia de Boas Práticas em Segurança da Informação, fruto do trabalho incansável e dedicado de nosso comitê e grupo de especialistas. Este guia tem como objetivo fornecer diretrizes claras e práticas para garantir a proteção adequada das informações dos Tribunais de Contas do Brasil.

Sabemos que vivemos em uma era digital, onde a informação se tornou um dos ativos mais valiosos de qualquer organização. Nesse contexto, a segurança da informação desempenha um papel crucial na manutenção da confidencialidade, integridade e disponibilidade desses dados. Portanto, é essencial estabelecer uma cultura de segurança sólida e implementar medidas eficazes para proteger nossos sistemas e informações sensíveis.

Com a crescente sofisticação das ameaças cibernéticas e a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), é imperativo que estejamos preparados para enfrentar os desafios que surgem em nosso ambiente tecnológico. O guia destaca a importância da conformidade com a LGPD e fornece orientações práticas para alcançar esse objetivo.

Ao adotar as diretrizes apresentadas, estaremos fortalecendo a postura de segurança de nossos Tribunais de Contas, protegendo informações sensíveis, mitigando riscos e garantindo a confiança dos cidadãos em nossas instituições.

Desejamos uma excelente leitura e implementação das boas práticas de segurança da informação!

Segurança da Informação

Coordenador do Grupo
Fábio Correa Xavier

Apresentação

O guia de Boas Práticas em Cibersegurança, tem como objetivo apresentar diretrizes para garantir a integridade, confidencialidade e disponibilidade das informações no contexto dos Tribunais de Contas. Reconhecendo a crescente importância da cibersegurança, este guia visa fortalecer a proteção dos dados e sistemas utilizados em nossas instituições, garantindo assim a continuidade de nossos trabalhos essenciais para a sociedade.

Vivemos em uma era digital, na qual a tecnologia desempenha um papel vital em nossas operações diárias. No entanto, com o avanço da tecnologia, surgem também ameaças cibernéticas cada vez mais sofisticadas e persistentes. Os Tribunais de Contas, responsáveis por assegurar a transparência, a responsabilidade e a eficiência na administração pública, tornaram-se alvos atrativos para os cibercriminosos em busca de informações sensíveis e vulnerabilidades para explorar.

A cibersegurança tornou-se, portanto, um requisito fundamental para a continuidade e o bom funcionamento dos Tribunais de Contas. A proteção de nossos dados, sistemas e processos é vital para garantir a confiança e a credibilidade perante a sociedade. Além disso, violações de segurança podem resultar em danos financeiros significativos, perda de informações confidenciais e até mesmo na interrupção de nossas atividades, impactando diretamente a efetividade de nossas análises e decisões.

A cibersegurança tornou-se, portanto, um requisito fundamental para a continuidade e o bom funcionamento dos Tribunais de Contas. A proteção de nossos dados, sistemas e processos é vital para garantir a confiança e a credibilidade perante a sociedade. Além disso, violações de segurança podem resultar em danos financeiros significativos, perda de informações confidenciais e até mesmo na interrupção de nossas atividades, impactando diretamente a efetividade de nossas análises e decisões.

Nesse contexto, o guia de Boas Práticas em Cibersegurança foi desenvolvido com base nas melhores práticas do mercado, incluindo referências a padrões reconhecidos, como NIST, framework CIS Controls, ISO 27001, ISC2, Gartner e IAPP. Essas práticas abrangem três pilares essenciais: tecnologias, processos e pessoas.

Ao seguir as diretrizes e boas práticas apresentadas neste guia, estaremos mais bem preparados para enfrentar os desafios da cibersegurança, proteger nossos ativos de informação e mitigar os riscos associados. Nosso objetivo é assegurar a continuidade de nossos trabalhos e manter a confiança da sociedade em nossa missão de garantir a eficiência e a responsabilidade na gestão dos recursos públicos.

INTRODUÇÃO

Ferramentas que fortalecem a segurança

A cibersegurança é uma área essencial para proteger os ativos digitais do setor público. Para garantir a segurança das informações e sistemas, é importante adotar boas práticas que envolvam Tecnologias, procedimentos e conscientização das pessoas. Este guia apresenta uma visão geral das melhores práticas de cibersegurança, independentemente de fabricantes, para ajudar a fortalecer a postura de segurança das Cortes de Contas.

"Se você colocar uma chave de baixo do tapete, permitirá que um ladrão encontre-a. Os cibercriminosos estão usando todas as ferramentas da tecnologia à sua disposição para hackear contas das pessoas. Se eles sabem que há uma chave escondida em algum lugar, eles farão de tudo para encontrá-la."

Tim Cook, CEO Apple

As práticas são divididas em 3 pilares. Por meio do pilar Tecnologias, exploraremos as ferramentas e soluções que podem fortalecer a segurança de nossos sistemas, como Next Generation Firewall (NGFW)s, sistemas de detecção de intrusões e antivírus. Já no pilar Processos, abordaremos a importância de políticas de segurança, gestão de vulnerabilidades, gestão de acesso e proteção de dados. E, por fim, destacaremos o papel crucial das pessoas no pilar Pessoas, fornecendo orientações sobre treinamentos, conscientização e práticas de segurança que todos devemos adotar.

1 TECNOLOGIAS

Ferramentas e soluções tecnológicas utilizadas para fortalecer a segurança dos sistemas e proteger as informações.

2 PROCESSOS

Políticas, procedimentos e práticas que visam proteger as informações e garantir a segurança dos sistemas. Isso incluia criação de políticas de segurança, a gestão de vulnerabilidades, a gestão de acesso e as práticas de proteção de dados.

3 PESSOAS

Conscientização e treinamento das pessoas envolvidos no ambiente organizacional.

PILAR 1

Tecnologias

O pilar tecnologias na cibersegurança abrange as ferramentas e soluções tecnológicas utilizadas para fortalecer a segurança dos sistemas e proteger as informações.

Isso inclui Next Generation Firewall (NGFW)s, sistemas de detecção de intrusões, antivírus, criptografia, autenticação de dois fatores, monitoramento de redes, entre outros. Essas tecnologias ajudam a identificar e mitigar ameaças, prevenir acessos não autorizados e garantir a integridade dos dados.

Defesa em profundidade

TECNOLOGIAS 1

Defesa em Profundidade é uma estratégia de cibersegurança que consiste em utilizar várias camadas de proteção para garantir a segurança dos sistemas e dados. Em outras palavras, em vez de depender de uma única medida de segurança, são implementadas diversas camadas de proteção que atuam em conjunto para impedir ou mitigar diferentes tipos de ameaças.

Um exemplo de defesa em profundidade é o uso de NextGeneration Firewall (NGFW)s, que são dispositivos de segurança colocados entre a rede interna e a internet. Eles monitoram o tráfego de dados, filtrando pacotes suspeitos e bloqueando o acesso não autorizado. Além disso, podem ser utilizados sistemas de detecção e prevenção de intrusões (IDS/IPS), que monitoram a rede em busca de atividades maliciosas e tomam medidas para bloquear ou responder a possíveis ataques.

Deve-se considerar também o uso desoluções WAF (Web Application Firewall). Esse recurso ajuda a proteger aplicações WEB de ataques vindos da Internet. Como a maioria dos sites são HTTPS, um IPS sem a inspeção SSL ativada não consegue prevenir ataques aos sites HTTPS.

A utilização de antivírus e antimalware. Esses programas realizam a verificação de arquivos em busca de ameaças conhecidas, como vírus, malware e ransomware. Ao identificar essas ameaças, eles agem para neutralizá-las e proteger o sistema.

Também é comum o uso de autenticação de dois fatores (2FA) ou autenticação multifator (MFA), que adiciona uma camada extra de segurança no acesso aos sistemas e dados. Nesse caso, além de inserir uma senha, é necessário fornecer uma informação adicional, como um código enviado por mensagem de texto ou um token gerado por um aplicativo no smartphone.

Esses são alguns exemplos de tecnologias que podem ser utilizadas na defesa em profundidade. A ideia principal é combinar diferentes medidas de segurança para garantir a proteção dos sistemas e dados em várias frentes, aumentando a segurança global e reduzindo as chances de uma violação ou ataque bem-sucedido.

TECNOLOGIAS 2

Detecção e resposta estendida

Detecção e Resposta Estendida, ou XDR (Extended Detection and Response), é uma abordagem avançada de cibersegurança que visa identificar e responder a ameaças de maneira mais eficiente e abrangente. Para entender melhor, vamos usar um exemplo.

Imagine que você tem uma casa e quer protegê-la contra invasões. Você instala uma câmera de segurança na entrada para monitorar qualquer atividade suspeita. Isso seria uma medida básica de detecção. No entanto, se alguém conseguisse passar pela câmera e entrar na casa, você não teria meios de resposta imediata.

Agora, vamos aplicar a ideia de Detecção e Resposta Estendida. Além da câmera de segurança na entrada, você também instala sensores de movimento em todas as janelas e portas. Se alguém tentar entrar pela janela dos fundos, os sensores de movimento detectam a intrusão e acionam um sistema de alarme sonoro. Além disso, você tem um serviço de segurança que recebe alertas de atividade suspeita em tempo real e envia uma equipe de segurança para verificar e responder à situação.

No contexto da cibersegurança, a Detecção e Resposta Estendida segue uma lógica similar. São implementadas diversas soluções de segurança, como sistemas de prevenção de intrusões, antivírus, monitoramento de rede, análise comportamental e inteligência artificial. Essas soluções trabalham juntas para detectar ameaças em diferentes pontos da infraestrutura de TI, como servidores, end points e dispositivos de rede.

Quando uma atividade suspeita é identificada, um alerta é gerado e encaminhado a uma equipe de segurança, que analisa a situação e toma medidas para conter a ameaça. Isso pode envolver o bloqueio do acesso ao sistema comprometido, a remoção do malware detectado ou a investigação adicional para entender a origem e o impacto da ameaça.

A Detecção e Resposta Estendida éuma abordagem mais abrangente, permitindo a correlação de eventos de segurança em vários pontos da infraestrutura e oferecendo uma visão mais completa do cenário de ameaças. Dessa forma, é possível responder de maneira mais eficiente e eficaz, reduzindo o tempo de detecção em inimizando os danos causados por um incidente de segurança.

TECNOLOGIAS 3

Confiança zero

Confiança Zero, ou Zero Trust, é uma abordagem de segurança cibernética que parte do princípio de que não se deve confiar cegamente em nenhum usuário, dispositivo ou rede, mesmo se estiverem dentro da infraestrutura de uma organização. Em vez disso, todas as tentativas de acesso aos recursos são verificadas e autenticadas continuamente, independentemente da origem.

... parte do princípio de que não se deve confiar cegamente em nenhum usuário, dispositivo ou rede, mesmo se estiverem dentro da infraestrutura de uma organização.

Vamos entender isso com um exemplo prático:

Imagine que você está em uma empresa e deseja acessar um arquivo confidencial armazenado em um servidor interno. No modelo tradicional de confiança, uma vez que você esteja conectado à rede interna, geralmente é permitido o acesso irrestrito a recursos sensíveis. Isso pressupõe que todos os usuários internos são confiáveis e não apresentam riscos.

Agora, vamos aplicar o conceito de Confiança Zero. Nesse cenário, antes de permitir o acesso ao arquivo confidencial, serão realizadas várias verificações e autenticações para confirmar sua identidade e determinar se você realmente precisa acessar esse arquivo. Essas verificações podem incluir autenticação multifator, análise de comportamento, verificação de credenciais, entre outros.

Outro exemplo seria o acesso a uma aplicação em nuvem. No modelo de Confiança Zero, em vez de conceder acesso contínuo e irrestrito a todos os usuários, mesmo depois de autenticados inicialmente, a abordagem de Confiança Zero exige a verificação de identidade e a autenticação em cada acesso, independentemente de estarem dentro ou fora da rede corporativa.

Para implementar a Confiança Zero, várias tecnologias podem ser utilizadas, como autenticação multifator, criptografia, controle de

acesso baseado em função (RBAC), micros segmentação de rede, políticas de controle de acesso e monitoramento contínuo de atividades suspeitas.

Um exemplo prático de Confiança Zero são ferramentas como o Google Authenticator ou Microsoft Authenticator, que geram códigos únicos que você precisa inserir para autenticar-se em determinados serviços. Mesmo que sua senha seja comprometida, o invasor não conseguirá acessar sua conta sem o código gerado pelo aplicativo.

Em resumo, a abordagem de Confiança Zero restringe o acesso apenas ao necessário, autentica continuamente os usuários e dispositivos, verifica a integridade e

a segurança dos sistemas, e adota uma postura de desconfiança em relação a qualquer acesso, mesmo que venha de dentro da organização. Isso ajuda a reduzir o risco de ataques, minimiza os danos em caso de violação e fortalece a segurança geral dos sistemas e dados.

Pesquisa

Como estão as cortes de contas?

dos **Tribunais de Contas utilizam soluções de confiança zero em seus ambientes tecnológicos.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

TECNOLOGIAS 4

Autenticação forte

Autenticação forte, também conhecida como autenticação de dois fatores(2FA) ou autenticação multifator (MFA), é um método de segurança que requer mais do que apenas uma senha para acessar um sistema, aplicativo ou conta online. Isso significa que além de digitar uma senha, é necessário fornecer uma informação adicional para provar sua identidade: "algo que você é (seu login), algo que você sabe (sua senha) e algo que você tem (seu aplicativo no smartphone)"

Vamos ver isso com exemplos práticos:

1 **Política de senha:** Uma política de senha forte é um conjunto de diretrizes que define requisitos para criar senhas robustas. Por exemplo, uma política pode exigir que as senhas tenham no mínimo oito caracteres, incluam letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, pode ser exigido que as senhas não sejam reutilizadas.

2 **Autenticação multifator (MFA):** Um exemplo comum de MFA é o uso de um aplicativo de autenticação no smartphone. Após inserir o nome de usuário e senha em um serviço online, você precisará fornecer um código gerado pelo aplicativo de autenticação. Esse código é único e muda a cada poucos segundos, garantindo uma camada extra de segurança. Outro exemplo de MFA é receber um código por mensagem de texto (SMS) no celular após inserir a senha. Ao inserir esse código, você completa o processo de autenticação.

O vetor de ataque inicial mais comum em 2022 foram credenciais roubadas ou comprometidas, responsáveis por 19% das violações no estudo, a um custo médio de us$ 4,50milhões.

Cost of a Data Breach Report 2022, IBM

A ideia por trás da autenticação forte é adicionar uma camada adicional de segurança para proteger suas contas contra acesso não autorizado, mesmo que alguém descubra sua senha. Mesmo que um invasor tenha acesso à sua senha, ele não poderá acessar sua conta

sem o segundo fator de autenticação.

A autenticação forte é amplamente utilizada em serviços online, como bancos, e-mails, redes sociais e aplicativos empresariais. Ela ajuda a prevenir ataques de hackers que tentam roubar informações pessoais ou acessar contas alheias.

Ao usar a autenticação forte, você aumenta significativamente a segurança de suas contas e reduz o risco de violação de dados

É importante destacar que a autenticação forte não é infalível, mas éum método muito mais seguro em comparação com o uso exclusivo desenhas. Por isso, é recomendável ativá-la sempre que disponível nos serviços que você utiliza, para proteger melhor suas informações pessoais e evitar o acesso não autorizado às suas contas.

Pesquisa

Como estão as cortes de contas?

dos **Tribunais de Contas utilizam autenticação forte com MFA.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PILAR 2

Processos

Procedimentos e práticas estabelecidos para garantir a efetividade e segurança das operações e atividades relacionadas à proteção de sistemas, dados e informações.

Foto: Luiz Gomes

PROCESSOS 1

Política de Segurança da Informação

A política de segurança da informação é um conjunto de diretrizes e regras estabelecidas por uma organização para proteger suas informações e sistemas contra ameaças e garantir sua confidencialidade, integridade e disponibilidade. Essa política define as responsabilidades dos funcionários, os procedimentos de segurança, as práticas recomendadas e as medidasde proteção a serem seguidas.

Vamos ver alguns exemplos de como a política de segurança da informação é importante:

1 **Senhas fortes:** Uma política de segurança da informação pode exigir que os funcionários criems enhas fortes para suas contas, com combinação de letras, números e caracteres especiais. Isso ajuda a proteger contra ataques de força bruta e a garantir que apenas pessoas autorizadas tenham acesso.

2 **Controle de acesso:** A política pode definir como os funcionários devem solicitar acesso asistemas e recursos, bem como os níveis de permissões que eles terão. Isso garante que apenas as pessoas certas tenham acesso aos recursos adequados e reduz o risco de acesso não autorizado.

3 **Classificação de informações:** A política pode estabelecer diretrizes sobre como classificar as informações, ou seja, categorizá-las de acordo com seu nível de sensibilidade. Isso ajuda a garantir que as informações confidenciais sejam tratadas com o devido cuidado e que apenas pessoas autorizadas possam acessá-las.

4 **Uso de dispositivos móveis:** Com a crescente utilização de dispositivos móveis, a política desegurança da informação pode estabelecer diretrizes para o uso seguro desses dispositivos. Isso inclui a instalação de softwares de segurança, a exigência de senhas para desbloqueio e o uso de conexões seguras ao acessar redes Wi-Fi públicas.

A política de segurança da informação é importante para proteger os ativos e as informações de uma organização. Ela ajuda a criar uma cultura de segurança, orienta os funcionários sobre as melhores práticas a serem seguidas e reduz os riscos de violações de segurança, perdas financeiras e danos à reputação da organização. Ter uma política de segurança da informação clara e bem implementada é essencial para garantir a proteção dos dados e a continuidade dos negócios.

PROCESSOS 2

Inteligência de ameaças cibernéticas

Inteligência de ameaças cibernéticas, ou Cyber Threat Intelligence (CTI), é um processo de coleta, análise e interpretação de informações sobre ameaças e ataques cibernéticos. Essas informações ajudam a compreenderas táticas, técnicas e procedimentos utilizados pelos criminosos cibernéticos, bem como suas motivações e objetivos.

Imagine que um Tribunal de Contas esteja sendo alvo de ataques cibernéticos frequentes. Por meio da inteligência de ameaças cibernéticas, é possível obter informações valiosas sobre as ameaças em potencial, como o tipo de malware usado, os vetores de ataque utilizados e as vulnerabilidades exploradas.

Com esses insights, a equipe de segurança pode implementar medidas preventivas e corretivas mais eficazes, protegendo a rede e os sistemas contra futuros ataques.

Além disso, a inteligência de ameaças cibernéticas permite a antecipação de possíveis ameaças. Ao monitorar fóruns de hackers, sites clandestinos e outras fontes de informações, é possível identificar atividades suspeitas que possam indicar um planejamento de ataque e mandamento. Essa antecipação permite que os Tribunais de Contas estejam preparados e adotem medidas preventivas antes que um ataque ocorra.

Outro aspecto importante da CTI é o compartilhamento de informações entre organizações. Os Tribunais de Contas podem se beneficiar de uma rede de inteligência de ameaças cibernéticas, onde diferentes instituições compartilham informações sobre ameaças e ataques em tempo real. Por exemplo, se um Tribunal de Contas recebe uma nova ameaça identificada por outra instituição, eles podem tomar medidas imediatas para se protegerem, mesmo antes de serem alvo direto.

Em resumo, a criação de uma rede de inteligência de ameaças cibernéticas entre as Cortes de Contas, fortalecerá a segurança cibernética e proteger as informações sensíveis e estratégicas dessas instituições.

Pesquisa

Como estão as cortes de contas?
Política de Segurança da Informação

dos **Tribunais de Contas possuem uma Política de Segurança da Informação formalmente implantada.**

Fonte: Pesquisa com secretários e diretores da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 3

Política de privacidade

A política de privacidade está na proteção dos direitos das pessoas em relação aos seus dados pessoais. Ela garante transparência na coleta eno uso dessas informações, permitindo que as pessoas tenham controle sobre seus dados e possam confiar que eles serão tratados de forma adequada e segura.

A política de privacidade é um conjunto de regras e diretrizes estabelecidas por uma organização para proteger as informações pessoais que são coletadas, armazenadas e utilizadas em suas atividades. Essa política define como os dados pessoais devem ser tratados, quem tem acesso a eles, como são protegidos e como as pessoas podem exercer seus direitos de privacidade. Vamos ver alguns exemplos de como a política de privacidade é importante, especialmente em conformidade com a Lei Geral de Proteção de Dados (LGPD):

...a política de privacidade é importante, especialmente em conformidade com a Lei Geral de Proteção de Dados.

1 **Consentimento para coleta de dados:** A política de privacidade pode incluir informações claras sobre quais dados pessoais são coletados e para quais finalidades. Por exemplo, um site de comércio eletrônico pode informara os usuários que coleta seu nome, endereço de entrega e informações de pagamento para processar e entregar os pedidos. É importante que os usuários concedam seu consentimento explícito para que seus dados sejam coletados e usados para essas finalidades específicas

2 **Direito de acesso e correção de dados:** A política de privacidade deve informar às pessoas seus direitos de acessar os dados pessoais que a organização possui sobre elas e corrigir quaisquer informações incorretas. Por exemplo, um banco deve permitir que seus clientes acessem suas informações financeiras e solicitem correções, caso detectem erros em seus registros.

3 Segurança dos dados pessoais: A política de privacidade deve descrever as medidas de segurança adotadas para proteger os dados pessoais contra acesso não autorizado, uso indevido ou divulgação. Isso inclui a implementação de tecnologias de segurança, como criptografia e Next Generation Firewall (NGFW)s, e a adoção de práticas adequadas de gerenciamento de riscos. Compartilhamento de dados com terceiros:

4 Compartilhamento de dados com terceiros: A política de privacidade deve explicar se os dados pessoais serão compartilhados com terceiros e sob quais condições. Por exemplo, uma empresa de marketing digital que compartilhadados com parceiros de publicidade deve informar aos usuários sobre esse compartilhamento e permitir que eles optem por não participar dessas práticas. A importância da política de privacidade está na proteção dos direitos das pessoas em relação aos seus dados pessoais. Ela garante transparência na coleta e no uso dessas informações, permitindo que as pessoas tenham controle sobre seus dados e possam confiar que eles serão tratados de forma adequada e segura. Além disso, a conformidade com a LGPD é fundamental para evitar multa se penalidades legais, garantindo que as organizações estejam em conformidade com as obrigações legais relacionadas à proteção de dados pessoais.

Foto de Tima Miroshnichenko

PROCESSOS 4

Política de governança em privacidade

Um programa de governança em privacidade é um conjunto de políticas, procedimentos e práticas implementadas por uma organização para garantir que a privacidade dos dados pessoais seja protegida de acordo com as regulamentações, como a Lei Geral de Proteção de Dados (LGPD).

Esse programa visa estabelecer uma estrutura de controle e responsabilidade, bem como promover a transparência e a conformidade com as obrigações legais.

Vamos ver alguns exemplos de como um programa de governança em privacidade é importante, especialmente para a conformidade com a LGPD:

1 **Nomeação de um encarregado de proteção de dados:** Uma organização pode designar um Encarregado, que é responsável por supervisionar a conformidade com as leis de proteção de dados, incluindo a LGPD. O Encarregado é o ponto de contato para questões relacionadas à privacidade e garante que as políticas e práticas adequadas sejam implementadas.

2 **Mapeamento e avaliação de dados pessoais:** Um programa de governança em privacidade envolve a identificação e classificação dos dados pessoais coletados e processados pela organização. Isso inclui entender como os dados são obtidos, armazenados, compartilhados e descartados. Essa análise permite que a organização avalie os riscos de privacidade e tome medidas adequadas para proteger esses dados.

3 **Implementação de medi-das de segurança:** Um programa de governança em privacidade exige a implementação de medidas de segurança apropriadas para protegeros dados pessoais. Isso inclui a utilização de criptografia, Next Generation Firewall (NGFW)s, controles de acesso e outras práticas de segurança para evitar o acesso não autorizado aos dados e protegê-los contra perdas ou vazamentos.

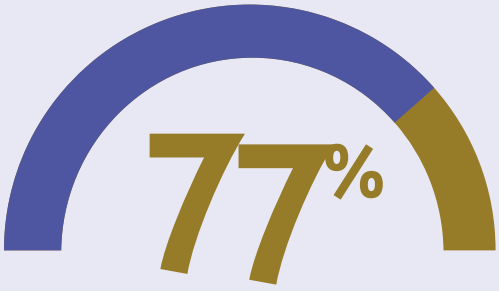
4 Treinamento e conscientização dos funcionários: É importante que os funcionários sejam treinados sobre as políticas e práticas de privacidade da organização. Isso ajuda a garantir que eles compreendam a importância da proteção de dados pessoais, saibam como lidar com essas informações adequadamente e estejam cientes das implicações legais relacionadas à privacidade.

A importância de um programa de governança em privacidade é garantir que a organização esteja em conformidade com as obrigações legais, protegendo a privacidade dos indivíduos cujos dados pessoais são coletados e processados. Além disso, um programa sólido de governança em privacidade fortalece a confiança dos clientes, aumenta a reputação da organização e reduz o risco de multas e sanções de correntes de violações de privacidade.

Pesquisa

Como estão as cortes de contas?

Gestão de Risco e Vulnerabilidade



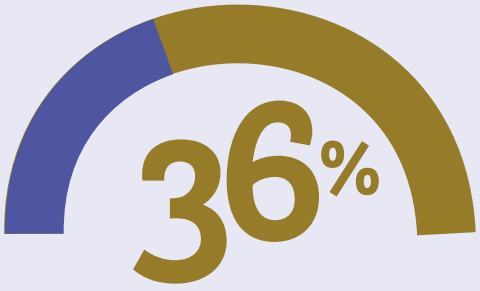
dos **Tribunais de Contas designaram um encarregado**

Fonte: Pesquisa com secretários e diretores da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

Pesquisa

Como estão as cortes de contas?

Gestão de Risco e Vulnerabilidade



dos **Tribunais de Contas realizam o inventário de dados pessoais**

Fonte: Pesquisa com secretários e diretores da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 5

Política de gerenciamento de identidade e acesso

A política de gerenciamento de identidade e acesso é um conjunto de diretrizes e procedimentos que uma organização implementa para controlar o acesso a recursos digitais, como sistemas, aplicativos e dados. Essa política é essencial para garantir que apenas as pessoas autorizadas tenham acesso aos recursos adequados, protegendo informações confidenciais e reduzindo o risco de violações de segurança.

Vamos ver alguns exemplos de como a política de gerenciamento de identidade e acesso é importante:

1 **Autenticação:** A política define como os usuários devem autenticar sua identidade para obter acesso aos recursos. Isso pode incluir o uso de senhas, autenticação de dois fatores (2FA) ou até mesmo biometria, como impressão digital ou reconhecimento facial. Por exemplo, ao acessar uma conta bancária online, é solicitado que o usuário insira uma senha e um código enviado para seu celular como medida de segurança adicional.

2 **Controle de acesso:** A política estabelece os níveis de permissões e privilégios concedidos a cada usuário com base em suas funções e responsabilidades. Por exemplo, um funcionário de um departamento financeiro pode ter acesso apenas a informações financeiras relevantes para sua função, enquanto um funcionário de recursos humanos terá acesso restrito a dados confidenciais de funcionários.

3 **Gerenciamento de contas de usuário:** A política define os procedimentos para criar, modificar e desativar contas de usuário. Isso inclui a revisão periódica das contas para garantir que apenas as contas ativas e necessárias estejam em uso. Por exemplo, quando um funcionário deixa a empresa, sua conta de usuário é desativada imediatamente para evitar acesso não autorizado após sua saída.

4 **Monitoramento de atividades:** A política inclui a implementação de sistemas de monitoramento para registrar e analisar as atividades dos usuários. Isso permite identificar atividades suspeitas ou incomuns que possam indicar tentativas de acesso não autorizado ou uso indevido de informações. Por exemplo, se alguém tentar fazer login repetidamente com senhas incorretas, isso pode acionar um alerta de segurança.

A importância da política de gerenciamento de identidade e acesso é garantir que apenas as pessoas certas tenham acesso aos recursos adequados, protegendo informações confidenciais e mitigando riscos de segurança.

Além disso, essa política ajuda a cumprir regulamentações de privacidade, como a Lei Geral de Proteção de Dados (LGPD), ao controlar o acesso a dados pessoais.

Ao implementar uma política eficaz de gerenciamento de identidade e acesso, as organizações reduzem o risco de violações de segurança, perda de dados e danos à reputação, promovendo um ambiente seguro e confiável.

PROCESSOS 6

Política de backup e recuperação de dados

A política de backup e recuperação de dados é um conjunto de diretrizes e procedimentos estabelecidos por uma organização para garantir a proteção e disponibilidade dos dados em caso de perda, corrupção ou danos. Essa política envolve a criação de cópias de segurança dos dados e a implementação de medidas para recuperá-los em situações de desastreou falhas de sistema.

Vamos ver alguns exemplos de como a política de backup e recuperação de dados é importante:

1 **Prevenção de perda de dados:** A política define como e com que frequência os dados serão copiados para locais seguros, como servidores de backup, discos externos ou serviços de nuvem. Essas cópias de segurança são essenciais para proteger os dados em caso de falhas de hardware, erros humanos, ataques cibernéticos ou desastres naturais.

Por exemplo, se um computador é danificado ou um arquivo é acidentalmente excluído, é possível recuperar os dados a partir do backup.

2 **Tempo de recuperação rápido:** A política estabelece a frequência com que os backups são atualizados e define metas para o tempo de recuperação dos dados. Isso significa que, em caso de perda de dados, é possível restaurá-los rapidamente e minimizar o impacto nos negócios. Por exemplo, se um servidor falhar, a restauração dos dados a partir de um backup recente pode permitir que a organização volte a operar em pouco tempo.

...Se você não pode se dar ao luxo de perder os dados, você não pode se dar ao luxo de não fazer backup.

Charles J. Orlando

3 Testes regulares de recuperação: A política inclui a realização de testes periódicos para garantir que os backups estejam funcionando corretamente e que os dados possam ser recuperados com sucesso. Esses testes simulam situações de falha e permitem identificar e corrigir possíveis problemas antes que ocorra uma perda real de dados. Por exemplo, uma organização pode restaurar um backup em um ambiente de teste para verificar se todos os dados estão completos e acessíveis.

4 Proteção contra ameaças cibernéticas: A política de backup também desempenha um papel importante na proteção contra ataques cibernéticos, como ransomware. Se os dados forem criptografados ou corrompidos por um ataque, a organização pode optar por restaurar os dados a partir de um backup anterior, eliminando a necessidade de pagar um resgate aos criminosos virtuais.

A importância da política de backup e recuperação de dados está na garantia da disponibilidade e integridade dos dados da organização. Ao implementar uma política eficaz, a organização está preparada para lidar com situações de perda de dados, minimizando o impacto nos negócios e protegendo informações valiosas. Além disso, apolítica de backup é fundamental para atender a requisitos regulatórios, como a Lei Geral de Proteção de Dados (LGPD), que exige a proteção adequadados dados pessoais.

Pesquisa

Como estão as cortes de contas?

dos **Tribunais de Contas possuem uma política de backup formalmente implantada.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 7

Política de resposta a incidentes

A política de resposta a incidentes é um conjunto de diretrizes e procedimentos estabelecidos por uma organização para lidar de forma eficaz com eventos de segurança cibernética, como ataques de hackers, violações de dados ou malware. Essa política define as etapas a serem seguidas para identificar, investigar, mitigar e recuperar-se de um incidente de segurança.

A importância da política de resposta a incidentes pode ser ilustrada por alguns exemplos e casos práticos:

1 **Detecção e resposta rápida:** A política estabelece protocolos para detectar e responder prontamente a incidentes de segurança. Isso inclui a implementação de sistemas de monitoramento de segurança, alertas em tempo real e equipes especializadas para lidar com incidentes. Por exemplo, se um funcionário receber um e-mail suspeito contendo um link malicioso, a política orienta o que deve ser feito para relatar o incidente e tomar medidas imediatas para mitigar o risco.

2 **Minimização de danos:** A política visa minimizar os danos causados por um incidente de segurança. Isso pode envolver o isolamento de sistemas comprometidos, a remoção de malware ou a restauração de backups de dados não afetados. Por exemplo,se um servidor for comprometido por um ataque de ransomware, a política orientará a ação para interromper a propagação do malware e restaurar os dados a partir de backups recentes.

3 **Investigação e análise:** A política deve definir os procedimentos para investigar e analisar os incidentes de segurança. Isso inclui coleta de evidências, análise forense e identificação das causas raiz dos incidentes. Essas informações são essenciais para entender as vulnerabilidades e implementar medidas corretivas para evitar incidentes futuros. Por exemplo, se ocorrer uma violação de dados em um sistema de e-commerce, a política de resposta a incidentes guiará a investigação para identificar como os invasores obtiveram acesso e implementar medidas para fortalecer a segurança do sistema.

4 Aprendizado contínuo: A política enfatiza a importância do aprendizado contínuo e da melhoria das práticas de segurança. Após um incidente, são realizadas avaliações pós-incidente para identificar lacunas e implementar ações corretivas. Isso contribui para fortalecer a postura de segurança da organização e reduzir o risco de futuros incidentes. Por exemplo, se ocorrer uma violação de dados que resulte na divulgação de informações pessoais dos clientes, a política orientará ações para notificar os clientes, a política orientará ações para notificar os clientes afetados, fortalecera segurança e revisar os processos para evitar incidentes semelhantes no futuro.

A importância da política de resposta a incidentes reside na capacidade de uma organização de identificar, responder e mitigar rapidamente os incidentes de segurança, minimizando os danos e protegendo seus ativos digitais. Recentemente, tem havido um aumento significativo no número de incidentes de segurança cibernéticaem todo o mundo. Segundo o Relatório de Ameaças Cibernéticas da Sonic Wallem 2021, foram registrados mais de 304 milhões de ataques de malware somente no primeiro semestre de 2021. Esses números destacam a necessidade crítica de uma política de resposta a incidentes robusta e eficiente para proteger as organizações contra as crescentes ameaças cibernéticas.

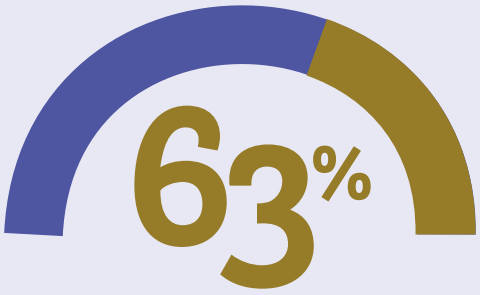
"Um plano de resposta a incidentes é o alicerce da cibersegurança eficaz. Ele permite que as organizações se preparem para incidentes de segurança cibernética, respondam de forma rápida e coordenada e minimizem os danos causados. Ter um plano bem estruturado e testado é crucial para proteger os ativos da organização e garantir a continuidade dos negócios.

Roberts, S. (2022). The Importance of an Effective Incident Response Plan in Cybersecurity. Journal of Cybersecurity Management, 8(3), 123-138.

Pesquisa

Como estão as cortes de contas?

Gestão de Risco e Vulnerabilidade



dos **Tribunais de Contas possuem uma política de resposta a incidentes.**

Fonte: Pesquisa com secretários e diretores da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 8

Gestão de vulnerabilidades

A gestão de vulnerabilidades é o processo de identificar, avaliar e trataras fraquezas nos sistemas e softwares de uma organização. Essas vulnerabilidades podem ser brechas de segurança que podem ser exploradas por cibercriminosos para comprometer a confidencialidade, integridade ou disponibilidade dos dados.

A importância da gestão de vulnerabilidades reside na proteção proativa contra possíveis ataques cibernéticos. Aqui estão alguns exemplos e casos práticos que destacam a importância desse processo:

A importância da política de resposta a incidentes pode ser ilustrada por alguns exemplos e casos práticos:

1 **Identificação de vulnerabilidades:** Por meio de varreduras de segurança automatizadas, é possível identificar vulnerabilidades conhecidas nos sistemas e softwares utilizados. Por exemplo, uma varredura pode revelar uma versão desatualizadade um software que possui uma vulnerabilidade conhecida, deixando o sistema suscetível a ataques. Ao identificar essas vulnerabilidades, as organizações podem tomar medidas para corrigi-las antes que sejam exploradas por atacantes.

2 **Ataques baseados em vulnerabilidades:** Muitos ataques cibernéticos exploram vulnerabilidades existentes nos sistemas. Um exemplo notório é o ransomware Wanna Cry, que se aproveitou de uma vulnerabilidade no protocolo SMB do Windows para se espalhar rapidamente. As organizações que não gerenciam adequadamentesuas vulnerabilidades estão em maior risco de serem vítimas desses ataques.

3 Patching e atualizações: A gestão de vulnerabilidades envolve a aplicação de patches de segurança e atualizações fornecidos pelos fabricantes de software. Essas atualizações muitas vezes corrigem vulnerabilidades conhecidas. Por exemplo, uma atualização de segurança pode corrigir uma vulnerabilidade crítica em um sistema operacional que poderia ser explorada para obter acesso não autorizado. A aplicação oportuna dessas correções é fundamental para manter a segurança dos sistemas.

4 Ameaças emergentes: As ameaças cibernéticas estão em constante evolução, e novas vulnerabilidades estão sendo descobertas regularmente. A gestão de vulnerabilidades permite que as organizações acompanhem as ameaças emergentes e apliquem contramedidas antes que sejam exploradas. Por exemplo, se uma nova vulnerabilidade é descoberta em um software amplamente utilizado, a gestão de vulnerabilidades permite que as organizações identifiquem sistemas afetados e apliquem as devidas correções.

Em resumo, a gestão de vulnerabilidades é fundamental para proteger os sistemas e dados de uma organização contra ameaças cibernéticas.

Ao identificar e corrigir vulnerabilidades conhecidas, aplicar patches e atualizações de segurança e acompanhar as ameaças emergentes, as organizações podem fortalecer sua postura de segurança e reduzir o risco de serem vítimas de ataques.

> ***O gerenciamento de vulnerabilidades é um processo contínuo, proativo e frequentemente automatizado que mantém seus sistemas de computador, redes e aplicativos corporativos protegidos contra ataques cibernéticos e violações de dados. Como tal, é uma parte importante de um programa geral de segurança.***
>
> Microsoft, disponível em https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Pesquisa

Como estão as cortes de contas?

dos **Tribunais de Contas não possui um programa de gerenciamento de risco e vulnerabilidades.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 9

Hardening de sistemas e dispositivos

O hardening de sistemas e dispositivos é o processo de fortalecer a segurança deles por meio da configuração adequada e da aplicação de medidas de proteção. Isso envolve desativar recursos desnecessários, aplicar atualizações de segurança, configurar corretamente permissões e autenticações, entre outras ações. A importância do hardening reside em mitigar riscos e reduzir a superfície de ataque. Aqui estão alguns exemplos e casos práticos que ilustram sua importância:

1 **Configuração de Next Generation Firewall:** Um Next Next Generation Firewall (NGFW) de segurança que controla o tráfego de rede. Ao configurá-lo adequadamente, bloqueando portas e restringindo o acesso não autorizado, é possível impedir que invasores acessem os sistemas internos da organização.

2 **Ataques de força bruta:** Muitos ataques cibernéticos tentam adivinhar senhas por meio de tentativas repetitivas. Ao implementar políticas de senha fortes, como exigir combinações de letras, números e caracteres especiais, e impor bloqueios após várias tentativas falhas, é possível mitigar o risco de ataques de força bruta bem-sucedidos.

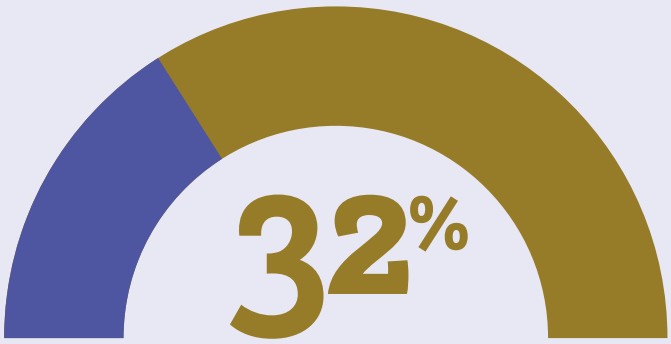
3 **Vulnerabilidades conhecidas:** Muitos ataques exploram vulnerabilidades conhecidas em sistemas e dispositivos desatualizados. Ao aplicar regularmente as atualizações de segurança fornecidas pelos fabricantes, é possível corrigir essas vulnerabilidades e reduzir a probabilidades e reduzir a probabilidade de um ataque bem-sucedido.

4 Incidentes de phishing: O phishing é uma técnica muito comum em que os atacantes tentam enganar os usuários para que revelem informações confidenciais, como senhas, por meio de e-mails ou sites falsos. Ao educar os usuários sobre como identificar e evitar golpes de phishing, é possível reduzir a probabilidade de um incidente de segurança causado por uma ação não intencional do usuário.

Em suma, o hardening de sistemas e dispositivos é crucial para fortalecer a segurança cibernética, reduzindo a exposição a ameaças. Ao configurar corretamente, aplicar atualizações e educar os usuários, é possível mitigar riscos e proteger as informações e os ativos da organização contra ataques maliciosos.

Pesquisa

Como estão as cortes de contas?



dos **Tribunais de Contas possuem uma política de hardening de software e hardware.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 10

Política de atualização de software

A política de atualização de software é um conjunto de diretrizes que estabelece a frequência e o processo para manter os softwares utilizados por uma organização atualizados com as versões mais recentes fornecidas pelos fabricantes. Isso inclui a aplicação de patches de segurança, atualizações de recursos e correções de bugs. A importância dessa política reside na proteção contra vulnerabilidades conhecidas e na garantia de que os softwares estejam funcionando corretamente.

Aqui estão alguns exemplos e casos práticos que ilustram sua importância:

1 **Vulnerabilidades conhecidas:** Os fabricantes de software lançam atualizações para corrigir vulnerabilidades de segurança em seus produtos. Por exemplo, se uma vulnerabilidade é descoberta em um navegador da web popular, uma atualização subsequente pode fechar essa brecha. Ao manter os softwares atualizados, a organização reduz o risco de ser vítima de ataques que exploram vulnerabilidades conhecidas.

2 **Ransomware e malware:** Muitos ataques cibernéticos, como o ransomware, exploram vulnerabilidades em softwares desatualizados para se infiltrar em sistemas e criptografar dados, exigindo um resgate para recuperá-los. Um exemplo notório é o ataque Wanna Cry, que se espalhou rapidamente em 2017, explorando uma vulnerabilidade no sistema operacional Windows. A atualização oportuna com os patches de segurança teria mitigado esse incidente.

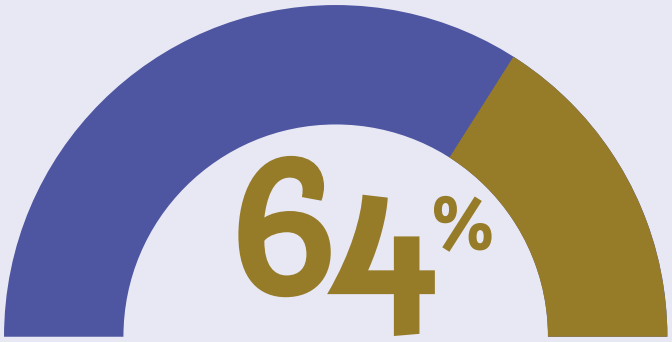
3 **Correções de bugs e melhorias:** As atualizações de software não se limitam apenas a correções de segurança. Elas também incluem correções de bugs e melhorias de desempenho e funcionalidade. Manter os softwares atualizados garante que os usuários tenham acesso a recursos aprimorados, menor probabilidade de erros e maior estabilidade geral do sistema.

4 Números de incidentes: Dados recentes destacam a importância de uma política de atualização de software. De acordo com o Relatório de Ameaças Cibernéticas da Sonic Wall em 2021, foram registrados mais de 13,2 milhões de tentativas de ataques de ransomware somente no primeiro trimestre do ano. Muitos desses ataques exploraram vulnerabilidades em softwares desatualizados. Esses números demonstram a necessidade crítica de manter os softwares atualizados para reduzir o risco de incidentes.

Em resumo, uma política de atualização de software é essencial para garantir a segurança e o desempenho adequados dos sistemas. Ao aplicar as atualizações fornecidas pelos fabricantes, a organização pode proteger-se contra vulnerabilidades conhecidas, reduzir a probabilidade de ataques cibernéticos bem-sucedidos e aproveitar as melhorias e correções oferecidas pelas atualizações.

Pesquisa

Como estão as cortes de contas?



dos **Tribunais de Contas possuem uma política de atualização de software.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PROCESSOS 11

Política de desenvolvimento seguro

Estabelecer uma política de desenvolvimento seguro é essencial para garantir a cibersegurança de uma organização. Essa política consiste em diretrizes e práticas que devem ser seguidas durante o processo de desenvolvimento de sistemas e aplicativos, com o objetivo de identificar e corrigir vulnerabilidades desde o início.

A importância dessa política reside no fato de que muitas falhas de segurança são introduzidas durante o processo de desenvolvimento. Ao negligenciar práticas seguras, como validação de entradas, tratamento adequado de erros e proteção de dados sensíveis, os desenvolvedores podem deixar brechas que podem ser exploradas por invasores.

Um exemplo comum de falha de segurança devido a uma política de desenvolvimento inadequada é a injeção de código, onde um invasor consegue inserir comandos maliciosos em um sistema através de uma entrada não validada. Isso pode resultar em acesso não autorizado, vazamento de informações confidenciais ou até mesmo comprometer todo o sistema.

Ao estabelecer uma política de desenvolvimento seguro, a organização estabelece diretrizes claras para os desenvolvedores seguirem, como a adoção de boas práticas de codificação, realização de testes de segurança e implementação de mecanismos de proteção. Isso ajuda a prevenir a introdução de vulnerabilidades e fortalece a segurança dos sistemas.

Além disso, uma política de desenvolvimento seguro promove uma cultura de segurança entre os desenvolvedores, tornando a segurança um aspecto integrante do processo de desenvolvimento. Isso resulta em sistemas mais robustos, protegidos contra ameaças cibernéticas e menos propensos a violações de dados.

Em resumo, estabelecer uma política de desenvolvimento seguro é essencial para o sucesso da cibersegurança, pois ajuda a prevenir a introdução de vulnerabilidades durante o processo de desenvolvimento e promove uma cultura de segurança entre os desenvolvedores. Isso resulta em sistemas mais seguros e protegidos contra ameaças cibernéticas, garantindo a integridade e confidencialidade das informações.

PROCESSOS 12

Inventário e controle de ativos e softwares institucionais

Estabelecer um inventário e controle de ativos e softwares institucionais é fundamental para o sucesso da cibersegurança. Imagine que uma empresa tenha vários computadores e dispositivos espalhados por diferentes departamentos. Sem um inventário preciso, seria difícil saber quantos e quais dispositivos estão conectados à rede, tornando difícil protegê-los adequadamente.

Com um inventário detalhado, é possível identificar todos os ativos e softwares utilizados pela organização. Isso inclui computadores, laptops, servidores, dispositivos móveis e até mesmo softwares específicos que são utilizados nos processos de trabalho. Ao conhecer todos os ativos, é possível implementar medidas de segurança adequadas, como atualizações de software, patches de segurança e monitoramento de atividades suspeitas.

Além disso, um inventário de ativos também ajuda na detecção e prevenção de ameaças, como dispositivos não autorizados conectados à rede ou softwares desatualizados que podem ser alvos fáceis para ataques.

Por exemplo, se um novo dispositivo desconhecido é conectado à rede, a equipe de segurança pode ser alertada e tomar medidas imediatas para avaliar a sua segurança e autenticidade.

Um caso prático seria o seguinte: uma empresa possui um inventário de ativos e, durante uma auditoria de segurança, foi identificado um dispositivo desconhecido conectado à rede. Ao investigar, foi descoberto que o dispositivo pertencia a um ex-funcionário que ainda tinha acesso aos sistemas. Graças ao inventário, a empresa foi capaz de agir rapidamente, revogar o acesso desse dispositivo e evitar um possível vazamento de informações sensíveis. Portanto, estabelecer um inventário e controle de ativos e softwares institucionais é essencial para garantir que todos os dispositivos e softwares utilizados pela organização sejam conhecidos, monitorados e protegidos adequadamente. Isso ajuda a minimizar os riscos de ataques cibernéticos, garantindo a segurança e integridade das informações da empresa.

PROCESSOS 13

Gestão de contas

Estabelecer um processo de Gestão de Contas é de extrema importância para a segurança cibernética de uma organização. Isso envolve a criação de um inventário de contas de serviço, a desabilitação de contas inativas e a restrição de privilégios de administrador.

Um inventário de contas de serviço consiste em identificar todas as contas criadas para permitir o funcionamento de serviços e sistemas dentro da organização. Essas contas muitas vezes possuem privilégios especiais e acesso a recursos sensíveis. Ao ter um inventário detalhado dessas contas, é possível garantir que apenas as contas necessárias estejam ativas e monitoradas.

Desabilitar contas inativas é essencial para reduzir o risco de acesso não autorizado. Por exemplo, se um funcionário deixa a empresa ou é transferido para outro departamento, é importante desabilitar sua conta de usuário para impedir que ela seja usada indevidamente. Isso evita que contas não utilizadas sejam alvo de ataques ou que sejam exploradas por usuários mal-intencionados.

Restringir privilégios de administrador é outro aspecto crucial da gestão de contas. Muitas vezes, as contas de administrador têm amplos poderes e acesso a áreas críticas do sistema. Limitar o número de contas de administrador e conceder privilégios apenas quando necessário reduz o risco de abuso ou comprometimento dessas contas. Isso significa que um invasor teria mais dificuldade em acessar informações confidenciais ou realizar ações prejudiciais na rede.

Um exemplo prático seria o seguinte: uma empresa percebeu que havia várias contas de serviço antigas que não eram mais necessárias, mas ainda estavam ativas. Um hacker identificou uma dessas contas desprotegidas e a utilizou para acessar informações confidenciais da empresa. Com um processo de Gestão de Contas adequado, a empresa poderia ter identificado e desabilitado essas contas inativas, minimizando o risco de acesso não autorizado.

Portanto, estabelecer um processo de Gestão de Contas, incluindo a criação de um inventário de contas de serviço, a desabilitação de contas inativas e a restrição de privilégios de administrador, é essencial para proteger os sistemas e informações da organização. Isso ajuda a reduzir o risco de ataques cibernéticos, garantindo que apenas as contas necessárias estejam ativas e que os privilégios sejam concedidos de forma controlada e monitorada.

PROCESSOS 14

Gestão de registros de auditoria

Estabelecer um processo de Gestão dos registros de auditoria é fundamental para garantir a segurança e a integridade dos sistemas e redes de uma organização. Logs são registros detalhados de eventos que ocorrem nos dispositivos e sistemas, como tentativas de acesso não autorizado, alterações de configuração e atividades suspeitas. Coletar, revisar e reter esses logs é essencial para identificar possíveis ameaças e realizar análises de segurança eficazes.

Por exemplo, imagine uma empresa que possui um processo de Gestão de registros de auditoria bem estabelecido. Durante a revisão dos logs, a equipe de segurança identifica uma série de tentativas de login não autorizadas em um servidor. Essa análise de log permitiu que a equipe agisse rapidamente, bloqueando o acesso do invasor e fortalecendo as medidas de segurança para evitar futuros ataques. Sem o registro adequado dessas atividades, seria difícil identificar essa ameaça e tomar medidas corretivas.

Além disso, a sincronização de tempo é um aspecto importante da Gestão de registros de auditoria. Ela garante que todos os dispositivos e sistemas estejam com seus relógios sincronizados, facilitando a correlação de eventos em diferentes registros. Por exemplo, se um evento suspeito é registrado em um servidor e a análise de logs em outro dispositivo indica uma atividade relacionada, a sincronização de tempo facilita a identificação dessa relação e a investigação apropriada.

A análise de logs também desempenha um papel crucial na detecção de anomalias e na identificação de atividades maliciosas. Por meio de ferramentas de análise de logs, é possível identificar padrões e comportamentos suspeitos que podem indicar uma possível violação de segurança. Por exemplo, uma análise de logs pode revelar uma série de tentativas de acesso a uma conta de usuário de forma repetitiva e em horários fora do comum, o que pode indicar uma tentativa de ataque. Portanto, estabelecer um processo de Gestão dos registros de auditoria, que inclua a coleta, revisão e retenção de logs, sincronização de tempo e análises de logs para detectar anomalias, é crucial para garantir a segurança dos sistemas e a identificação de possíveis ameaças. Essa prática ajuda a proteger a organização contra ataques cibernéticos, fornecendo uma visão clara das atividades realizadas e facilitando a resposta efetiva a incidentes de segurança.

PILAR 3

Pessoas

O pilar "pessoas" é um dos aspectos mais críticos da cibersegurança. Ele se refere às pessoas envolvidas na organização, como funcionários, usuários e administradores de sistemas.

A importância desse pilar está no fato de que as pessoas podem ser tanto a primeira linha de defesa contra ameaças quanto um ponto de vulnerabilidade se não estiverem devidamente treinadas e conscientizadas sobre as melhores práticas de segurança.

As ações das pessoas podem ter um impacto significativo na segurança dos sistemas e dados.

A seguir, são abordados alguns pontos-chave que ilustram a importância do pilar pessoas em cibersegurança.

PESSOAS 1

Conscientização e treinamento

A conscientização e o treinamento em cibersegurança são essenciais para ajudar as pessoas a entenderem os riscos e adotarem práticas seguras no uso da tecnologia. É importante destacar a importância desses dois elementos para ilustrar seu impacto na segurança e fornecer alguns exemplos e casos práticos.

A conscientização em cibersegurança envolve educar as pessoas sobre os riscos e as melhores práticas para proteger seus dados e informações pessoais. Isso inclui entender ameaças como phishing, em que um atacante tenta obter informações confidenciais por meio de mensagens enganosas. Por exemplo, alguém pode receber um e-mail que aparenta ser de um banco, solicitando informações pessoais. Com a conscientização adequada, as pessoas aprenderiam a identificar tais tentativas de phishing e não compartilhariam informações confidenciais.

O treinamento em cibersegurança capacita as pessoas com conhecimentos técnicos e habilidades práticas para proteger seus dispositivos e dados.

Isso pode incluir o uso de senhas fortes, a atualização regular de software e a adoção de medidas de segurança como autenticação de dois fatores (MFA). Por exemplo, uma pessoa que recebe treinamento em cibersegurança saberia que é importante usar senhas exclusivas para cada conta online e evitar senhas óbvias, como "123456". Isso ajudaria a evitar que sua conta seja comprometida em caso de vazamento de senhas em um site.

A importância da conscientização e do treinamento em cibersegurança é evidente nos casos em que a falta desses elementos resulta em violações de segurança. Por exemplo, um funcionário que não foi treinado adequadamente pode abrir um e-mail de phishing e divulgar informações confidenciais, resultando em uma violação de dados da empresa. Além disso, indivíduos que não estão conscientizados sobre a importância de atualizar regularmente o software podem ficar vulneráveis a ataques que exploram vulnerabilidades conhecidas em sistemas desatualizados.

Em resumo, a conscientização e o treinamento em cibersegurança são fundamentais para proteger-se contra ameaças online. Eles ajudam as pessoas

a reconhecer e evitar ataques, adotar práticas seguras e proteger seus dados pessoais. Ao investir em conscientização e treinamento em cibersegurança, as organizações e os indivíduos podem reduzir significativamente os riscos de violações e ataques cibernéticos.

Um programa eficaz de treinamento em segurança cibernética deve ser adaptado às necessidades específicas da instituição, levando em consideração o público-alvo, o tamanho e requisitos. Algumas dicas para criar um programa de treinamento de sucesso seriam:

Mantenha-o relevante

Certifique-se de que o treinamento seja relevante para as funções e responsabilidades de seus funcionários, bem como para as ameaças de segurança cibernética que eles provavelmente enfrentarão. Isso ajudará a garantir que os tópicos abordados sejam significativos e interessantes, para que os funcionários prestem atenção e retenham as informações.

Inclua treinamento prático

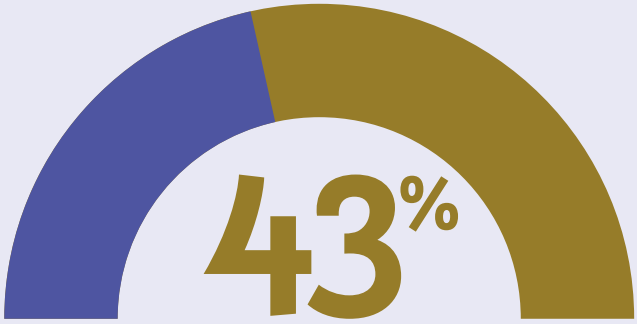
O treinamento prático é uma parte importante de qualquer programa de segurança cibernética. Isso pode incluir simulações ou exercícios para que os funcionários entendam as aplicações do mundo real dos tópicos que estão aprendendo.

Torne o treinamento divertido

Tornar o treinamento de segurança cibernética divertido e envolvente pode ajudar a aumentar a retenção e garantir

Pesquisa

Como estão as cortes de contas?



dos **Tribunais de Contas possuem uma equipe dedicada para tratar a segurança da informação.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

que os funcionários participem ativamente do processo de aprendizado. Você pode incorporar elementos de jogos, vídeos ou outras atividades interativas para tornar a sessão mais agradável.

Torne o treinamento acessível

Os funcionários devem poder acessar os materiais de treinamento sempre que precisarem, então considere fornecer módulos online ou webinars que os funcionários possam fazer em seu próprio ritmo. Além disso, certifique-se de que o treinamento esteja disponível em vários idiomas, se necessário.

Forneça treinamento e atualizações regulares

As ameaças de segurança cibernética estão em constante evolução, portanto, os funcionários devem ser treinados regularmente sobre os mais recentes protocolos e técnicas de segurança. Além disso, considere fornecer cursos de atualização conforme necessário para garantir que os funcionários se mantenham atualizados sobre os últimos desenvolvimentos em privacidade e segurança de dados.

Incentive comentários

É importante obter feedback dos funcionários sobre a eficácia do treinamento em segurança cibernética. Isso pode ajudá-lo a identificar quaisquer lacunas no conhecimento ou áreas que precisam ser abordadas mais detalhadamente.

Pesquisa

Como estão as cortes de contas?

dos **Tribunais de Contas possuem treinamento e conscientização constante.**

Fonte: Pesquisa com secretários e diretores de tecnologia da informação, no âmbito do Comitê de Tecnologia do IRB jun/23

PESSOAS 2

Engajamento da alta administração

O engajamento e apoio da alta administração são fundamentais para o sucesso da cibersegurança em uma organização. Isso significa que os conselheiros e a alta direção devem estar comprometidos em promover e implementar práticas de segurança eficazes.

Vamos tentar ilustrar a importância do engajamento e apoio da alta administração por meio de exemplos e casos práticos.

O engajamento da Alta Administração envolve a demonstração de liderança no estabelecimento de uma cultura de segurança cibernética e a alocação adequada de recursos para sua implementação. Quando os líderes mostram preocupação com a segurança cibernética, os funcionários são mais propensos a adotar práticas seguras. Por exemplo, se um conselheiro promove a importância da segurança cibernética em discursos e reuniões, isso cria um ambiente propício para que os servidores valorizem e adotem medidas de segurança.

O apoio da Alta Administração também se reflete na implementação de políticas e procedimentos robustos de cibersegurança. Isso inclui a alocação de orçamento para contratar especialistas em cibersegurança, a implementação de sistemas de proteção avançados e a realização de auditorias regulares para identificar e corrigir vulnerabilidades.

Por exemplo, se a Alta Administração investe em um sistema de detecção de intrusões que monitora e alerta sobre atividades suspeitas na rede, isso pode ajudar a evitar ataques cibernéticos e proteger os ativos da organização.

A importância do engajamento e apoio da Alta Administração pode ser observada em casos em que a falta desses elementos resultou em falhas de segurança. Por exemplo, se a Alta Administração não prioriza a segurança cibernética e não fornece recursos adequados para sua implementação, a organização pode ficar vulnerável a ataques como ransomware, em que os dados são sequestrados e exigidos resgate. Além disso, a falta de apoio da Alta Administração pode levar a uma falta de conscientização e priorização da segurança cibernética em toda a organização, o que aumenta o risco de violações de dados e prejuízos financeiros.

Em resumo, o engajamento e apoio da alta administração são essenciais para o sucesso da cibersegurança. Eles estabelecem uma cultura de segurança, alocam recursos para a implementação de medidas de proteção e garantem que a segurança cibernética seja uma prioridade em toda a organização. Ao demonstrar liderança e investir em segurança cibernética, os líderes ajudam a proteger os ativos e a reputação da organização, reduzindo os riscos de violações e ataques cibernéticos.

PESSOAS 3

Fornecedores

Estabelecer requisitos de segurança cibernética para fornecedores é essencial para garantir a proteção dos dados e a conformidade com a LGPD (Lei Geral de Proteção de Dados). Isso significa que ao contratar um fornecedor de serviços ou produtos que envolvam o tratamento de dados pessoais, é necessário exigir que eles adotem medidas de segurança adequadas.

Ao estabelecer requisitos de segurança cibernética para fornecedores, a empresa pode garantir que eles tenham controles adequados para proteger os dados pessoais. Isso pode incluir medidas como criptografia de dados, controle de acesso, monitoramento de atividades suspeitas e auditorias regulares. Além disso, é importante que a empresa revise periodicamente a conformidade do fornecedor com esses requisitos e exija evidências de conformidade, como certificações de segurança.

A importância de tais requisitos para fornecedores pode ser observada em casos em que a falta dessa prática resultou em violações de dados.

Por exemplo, se uma empresa terceiriza o processamento de folha de pagamento para um fornecedor que não adota medidas adequadas de segurança, os dados sensíveis dos funcionários podem ser comprometidos. Isso poderia resultar em roubo de identidade ou fraude financeira, além de consequências legais e reputacionais negativas para a empresa.

... é importante que a empresa revise periodicamente a conformidade do fornecedor...

Em resumo, a importância de tais requisitos para fornecedores é crucial para proteger os dados pessoais e garantir a conformidade com a LGPD. Ao exigir que os fornecedores adotem medidas de segurança adequadas, a empresa reduz os riscos de violações de dados e protege a privacidade de seus clientes. Essa prática é uma parte essencial da gestão de riscos e da construção de relacionamentos confiáveis com fornecedores, promovendo a segurança cibernética e a conformidade com as leis de proteção de dados.

Regra de Pareto da cibersegurança

1 Manter softwares atualizados as 10 vulnerabilidades mais exploradas para o comprometimento de sistemas e redes governamentais são conhecidas e possuem correçõe, algumas há mais de 5 anos."

2 Hardening de sistemas e dispositvos especialmente para mudar configurações de fábrica alterando, por exemplo, usuário e senhas amplamente conhecidas e desabilitando protocolos inseguros ou não utilizados

3 Melhorar processo de autenticação sistemas que utilizam apenas senhas como forma de autenticação são alvos mais fáceis para golpes digitais. Uma forma de melhorar a segurança dos sistemas é utilizar múltiplos fatores de autenticação


Foto de cottonbro studio

Fonte: Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques

Mensagem Final

Este guia foi elaborado com o objetivo de fornecer orientações claras e abrangentes para a proteção dos dados e sistemas utilizados nesses órgãos. Ao seguir as práticas aqui apresentadas, os Tribunais de Contas estarão fortalecendo sua capacidade de lidar com ameaças cibernéticas, garantindo a confidencialidade, integridade e disponibilidade das informações críticas.

Por meio de uma abordagem holística, este guia abrange os três pilares fundamentais da segurança da informação: tecnologias, processos e pessoas. São apresentadas as melhores práticas do mercado, alinhadas com as diretrizes do NIST, framework CIS Controls, ISO 27001, IAPP, ISC2, grandes players do mercado e referências do Gartner.

A conscientização e o treinamento dos servidores são destacados como fatores fundamentais para a proteção efetiva das informações. A importância de uma política de privacidade sólida, em conformidade com a LGPD, é ressaltada, assim como a necessidade de um programa de governança em privacidade para garantir o devido tratamento dos dados pessoais.

Adicionalmente, são abordados tópicos essenciais, como a importância da resposta a incidentes, gestão de vulnerabilidades, hardening de sistemas e dispositivos, política de atualização de software e backup de dados. Essas práticas visam mitigar riscos e reduzir a possibilidade de incidentes prejudiciais, como violações de dados, interrupção de serviços e danos à reputação.

Lembre-se de que a segurança da informação é uma jornada contínua. Ameaças evoluem constantemente, e é necessário manter-se atualizado e adaptar as práticas de segurança conforme necessário.

Desejamos sucesso na implementação e na adoção das boas práticas de segurança da informação, fortalecendo a resiliência e a confiança dos Tribunais de Contas do Brasil.

Proteger as informações é proteger o coração da organização.

Vivemos em uma era digital, na qual a tecnologia desempenha um papel vital em nossas operações diárias. No entanto, com o avanço da tecnologia, surgem também ameaças cibernéticas cada vez mais sofisticadas e persistentes. Os Tribunais de Contas, responsáveis por assegurar a transparência, a responsabilidade e a eficiência na administração pública, tornaram-se alvos atrativos para os cibercriminosos em busca de informações sensíveis e vulnerabilidades para explorar.

Instituto Rui Barbosa
A Casa do Conhecimento dos Tribunais de Contas