10 PASSOS PARA ESTABELECER **POLÍTICAS E PRÁTICAS DE SEGURANÇA CIBERNÉTICA** SÓLIDAS NA SUA EMPRESA

Os ataques cibernéticos cresceram 94% no Brasil no último ano. Foram mais de **31,5 bilhões de tentativas de golpes virtuais**. Empresas públicas e privadas fazem parte da lista de alvos, sendo o **setor financeiro** um dos mais afetados. Em âmbito global, isso representa mais de 82% do cibercrime. E aqui no Brasil, uma das explicações para o aumento de incidentes ainda é o baixo investimento em cibersegurança, representando hoje um grande fator de risco.

Novos conceitos, **como a Internet dos Sentidos, uso de Inteligência Artificial, implementação de 5G, IoT e novas tecnologias**, possibilitam que os cibercriminosos implementem seus ataques, tornando-os mais complexos.

Essas ameaças, que antes exigiam habilidades, conhecimentos e recursos sofisticados, agora estão disponíveis no submundo da internet, **a Deep e a Dark Web**, com venda de pacotes de Ransomware a partir de US$220.

Esses incidentes permanecem em níveis máximos, sem evidência de desaceleração no mundo. As novas variantes habilitadas por Ransomware-as-a-Service (RaaS) **colocam em risco a segurança da informação das organizações**. Por isso, a conscientização e políticas em segurança cibernética são fundamentais para evitar que os criminosos obtenham acesso aos dados e sistemas das empresas.

COMO AS EMPRESAS DEVEM SE PREPARAR?

De acordo com o **National Cyber Security Centre** (NCSC), definir e comunicar as políticas de segurança da informação para sua organização é fundamental.

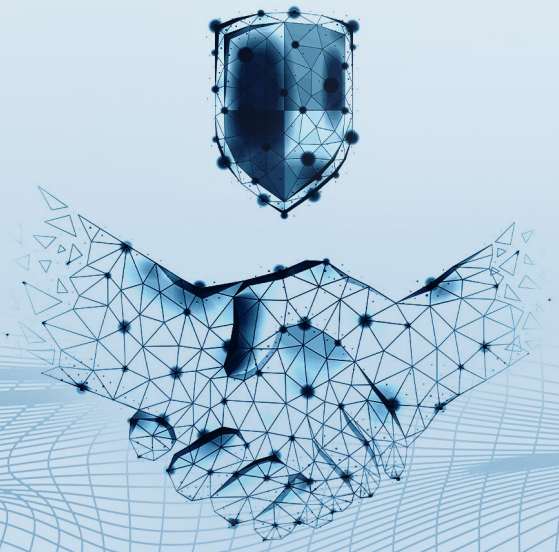
Um plano de segurança cibernética pode ser definido como **um documento que contém informações sobre todas as políticas, procedimentos e contramedidas de segurança que uma empresa adota**.

O seu objetivo é garantir a integridade das operações e a segurança dos ativos da empresa.

A ISO é uma boa fonte para que as empresas aperfeiçoem suas políticas de segurança. Mesmo que informalmente, todos adotam algum tipo de regra ou recomendações para acessar sites, receber/enviar e-mails, criar senhas de acesso, ter cópia de segurança etc.

As corporações mais bem preparadas buscam as melhores práticas para Sistema de Gestão de Segurança da Informação (SGSI) com base, por exemplo, nas **certificações ISO 27001 e 27002**.

Para manter sua empresa protegida de ataques virtuais, siga essas 10 recomendações:



1 – TUDO COMEÇA COM UM PLANEJAMENTO

Sua empresa só é capaz de **reconhecer os cenários de riscos, interpretá-los e procurar a solução certa** para se proteger, quando tem visibilidade completa da superfície de ataque.

Sabemos que não é fácil **proteger aquilo que não se pode ver**, por isso é preciso estar atento aos impedimentos que sua organização pode enfrentar ao tentar implementar sistemas de segurança.

O planejamento é o primeiro passo, desde a sua abertura (plano de negócio) até a elaboração de uma estratégia de segurança cibernética.

Antes de qualquer ação, **levante todos os tipos de dados que a empresa possui**, suas portas de entrada, quem e como as pessoas têm acesso, onde, a forma que são armazenados e quais os maiores riscos. Cada departamento também deve ter um inventário de todos os equipamentos e dispositivos que são conectados à rede corporativa.

2 - INVISTA EM TECNOLOGIAS DE SEGURANÇA CIBERNÉTICA

Com tantas novidades no mercado, escolher a melhor tecnologia para a segurança da sua empresa se torna um desafio. Mas, **é importante considerar algumas essenciais** e que podem fazer a diferença no seu negócio:

Firewall – visa proteger a rede de ataques externos, bloqueando IPs desconhecidos de acessarem as redes;

IDS/IPS – complementam a função do Firewall. O IDS rastreia qualquer tipo de anormalidade na rede, como downloads sucessivos, por exemplo. Aí, entra o IPS, que bloqueia os IPs que estão causando este evento;

Webfilter – é uma ferramenta de controle de conteúdo que restringe o que pode ou não ser acessado pelos usuários, evitando que programas maliciosos infectem a rede corporativa.

Antivírus – são softwares que evitam que malwares invadam os sistemas, mas precisam ser instalados de máquina em máquina, e serem atualizados constantemente;

Backup – Basta uma falha no sistema, um ataque cibernético ou um simples erro humano, para colocar tudo de mais importante a perder. O backup em nuvem pode ser a salvação da sua empresa, protegendo a integridade das informações, de configurações, banco de dados e arquivos dos usuários

Implemente auditoria de segurança e testes de penetração

A auditoria de segurança e os testes de penetração são medidas fundamentais para garantir a integridade dos dados e a privacidade. A implementação dessas práticas pode ajudar a detectar e corrigir vulnerabilidades antes que elas possam ser exploradas, protegendo a organização contra ataques mal-intencionados.

Ação extra:

A plataforma Vision 3.0 da ISH é uma solução integrada de gerenciamento de segurança da informação que ajuda as empresas a monitorar, identificar e responder a possíveis ameaças cibernéticas em tempo real.

Oferece uma visão abrangente das ameaças de segurança cibernética em toda a rede da organização, usando recursos como monitoramento de eventos de segurança, detecção de ameaças, resposta a incidentes, gerenciamento de vulnerabilidades e conformidade regulatória.

SAIBA MAIS AQUI

3 - TREINE OS FUNCIONÁRIOS

Os riscos cibernéticos estão presentes em várias atividades operacionais e podem causar **prejuízos financeiros e de reputação** para as empresas.

Por isso, é fundamental que todos os colaboradores estejam conscientes da importância da segurança cibernética e sejam incentivados a contribuir com sugestões e ideias. É importante que as **políticas de segurança cibernética sejam difundidas em todas as áreas da empresa** e incorporadas nas práticas diárias de trabalho.

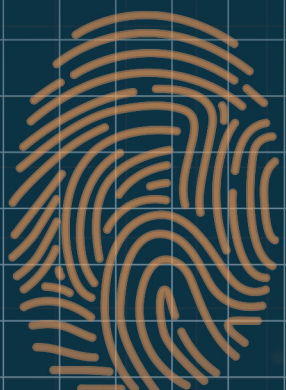
Para que isso aconteça, é essencial que **os C-Levels liderem a cultura de segurança cibernética**, garantindo que todos os colaboradores recebam treinamento adequado. Além disso, é importante que as políticas sejam revisadas e atualizadas regularmente para acompanhar as mudanças no cenário de ameaças.

4 - IMPLEMENTE CRIPTOGRAFIA NA REDE E NOS DISPOSITIVOS

A criptografia é uma técnica importante para proteger a identidade e os dados dos usuários contra invasões e roubo de informações. Ela cria uma **chave única** que permite que somente **a pessoa autorizada** tenha acesso aos dados criptografados. Isso ajuda a garantir a **privacidade** e a segurança dos dados pessoais dos usuários, além de proteger o conteúdo de arquivos e mensagens trocadas.

O uso de criptografia ganhou importância com a **LGPD (Lei Geral de Proteção de Dados)**, que prevê multas pesadas para quem desrespeitar a privacidade de dados pessoais. Além disso, é comum que cibercriminosos sequestrem os dados de empresas e ameacem divulgar as informações na internet caso o resgate não seja pago.

Qualquer dispositivo que fica online, desde celulares, tablets e até computadores, precisam ser criptografados. Isso ajuda a prevenir invasões de hackers e a proteger os dados pessoais dos usuários. É importante lembrar que a segurança cibernética é responsabilidade de todos, desde os usuários individuais até as empresas terceirizadas que armazenam e processam dados pessoais.



5 – GERENCIAMENTO DE IDENTIDADE E ACESSO

Da mesma forma que não é qualquer pessoa que pode entrar na empresa, o mesmo deve ocorrer na rede corporativa.

O **IAM (Identity Access Management)** é um controle básico de segurança da nuvem que autentica usuários e regula o acesso a sistemas, redes e dados.

O processo envolve a validação de identidades de usuários e seus direitos de acesso associados a um sistema específico. As soluções IAM fornecem **ferramentas para gerenciar as identidades digitais dos usuários e garantir o acesso adequado** aos recursos da empresa. Permitindo assim, que os administradores rastreiem as atividades, criem relatórios e apliquem políticas para garantir a conformidade.

O IAM possui três pilares:

IGA (Identity Governance Administration): automatiza a criação, o gerenciamento e certificação de contas de usuário, funções e direitos de acesso para o funcionário de uma organização. Ele permite uma maior visibilidade das identidades de uma pessoa, além de seus privilégios de acesso;

AM (Access Management): controla o acesso a aplicativos, serviços e infraestrutura locais e baseados em nuvem. O AM garante que somente usuários selecionados tenham acesso autorizado a recursos específicos durante um determinado período;

PAM (Privileged Access Management): monitora, detecta e impede o acesso privilegiado não autorizado a recursos críticos como, por exemplo, a conta de um administrador de domínio, já que elas controlam todas as estações de trabalho e servidores de uma empresa.

Ação extra:

Para que o gerenciamento de identidade e acesso seja eficaz, é necessário atentar-se a alguns **riscos**, como a automação e processo insuficiente, falta de treinamento gerencial e auditoria, entre outros.

As soluções de Identity and Access Management (IAM) são essenciais para **gerenciar e controlar o acesso dos usuários aos sistemas e aplicativos, permitindo a identificação e autenticação segura e eficiente** dos usuários, prevenindo ataques e protegendo a privacidade dos dados pessoais. O **ISH Board** oferece uma solução completa de segurança cibernética que garante a conformidade e proteção dos dados corporativos e dos usuários.

SAIBA MAIS AQUI

6 - GERENCIE O ANTIVÍRUS

O antivírus corporativo consiste em um software de proteção contra ameaças cibernéticas **com mais recursos e robustez** do que as soluções para dispositivos pessoais (antivírus residenciais) ou versões gratuitas. Eles são gerenciados e constantemente atualizados.

Esses programas foram desenvolvidos para **detectar e remover ameaças**, como vírus eletrônicos, worms, cavalos de troia etc. O antivírus gerenciado previne o acesso a sites suspeitos, evitando roubo de informações, invasões e protegendo todos os tipos de dispositivos conectados na infraestrutura corporativa, como notebooks, desktops, servidores e dispositivos móveis.

As regras de proteção podem ser **definidas e aplicadas para toda a rede de uma só vez**, o que reduz os custos de manutenção e agiliza todo o processo.

Um bom antivírus corporativo é capaz de:

- Identificar e remover os vírus eletrônicos;
- Impedir os downloads de programas ilegais ou uso de programas sem licenciamento legítimo;
- Abertura de anexos de e-mail suspeito;
- Uso de unidades removíveis infectadas (como dispositivos USB);
- Acesso a páginas web infectadas;
- Cliques em links maliciosos;
- Anúncios web infectados com malware.

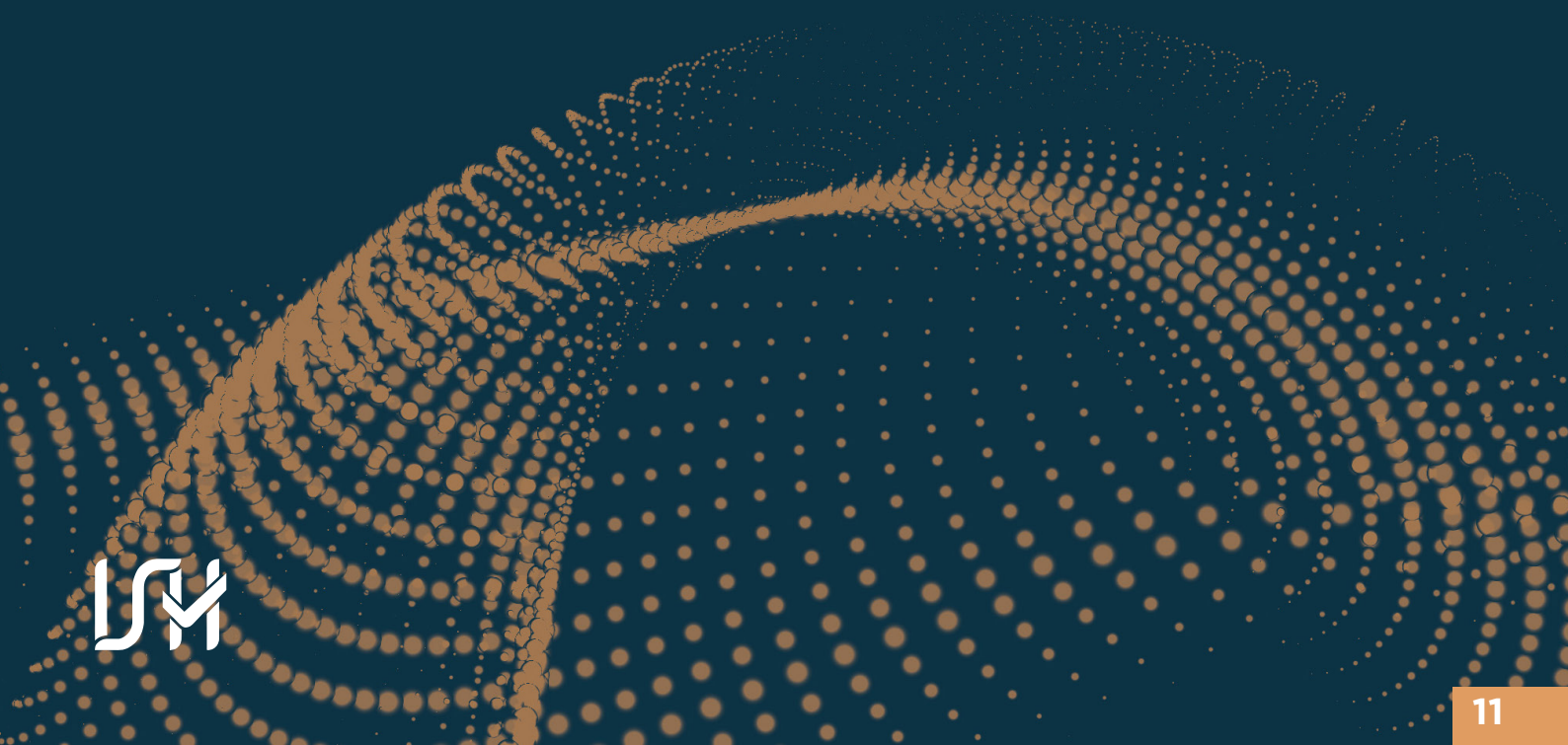
7 - GERENCIAMENTO DE PATCHES E ATUALIZAÇÕES

Em inglês, patch significa **remendo**. Basicamente, são as pequenas **atualizações** lançadas pelo fornecedor de software para a **correção de pontos de segurança** ou qualquer outro item dentro do sistema que vá garantir o melhor funcionamento e segurança.

A **Microsoft** e outros fabricantes disponibilizam mensalmente um conjunto de correções na segunda terça-feira do mês, chamado **Patch Tuesday**. Em situações críticas, uma correção pode ocorrer a qualquer momento, dependendo de sua gravidade.

O ideal é que, sempre que for disponibilizado um patch, seja de correção ou uma simples atualização, **ele seja aplicado imediatamente**.

É preciso lembrar que não apenas o sistema operacional trabalha com atualizações, mas também todos os outros softwares. Dependendo da complexidade do ambiente de TI, **a empresa precisará de ajuda de especialistas, como um provedor de Serviços Gerenciados de Segurança (MSSP).**



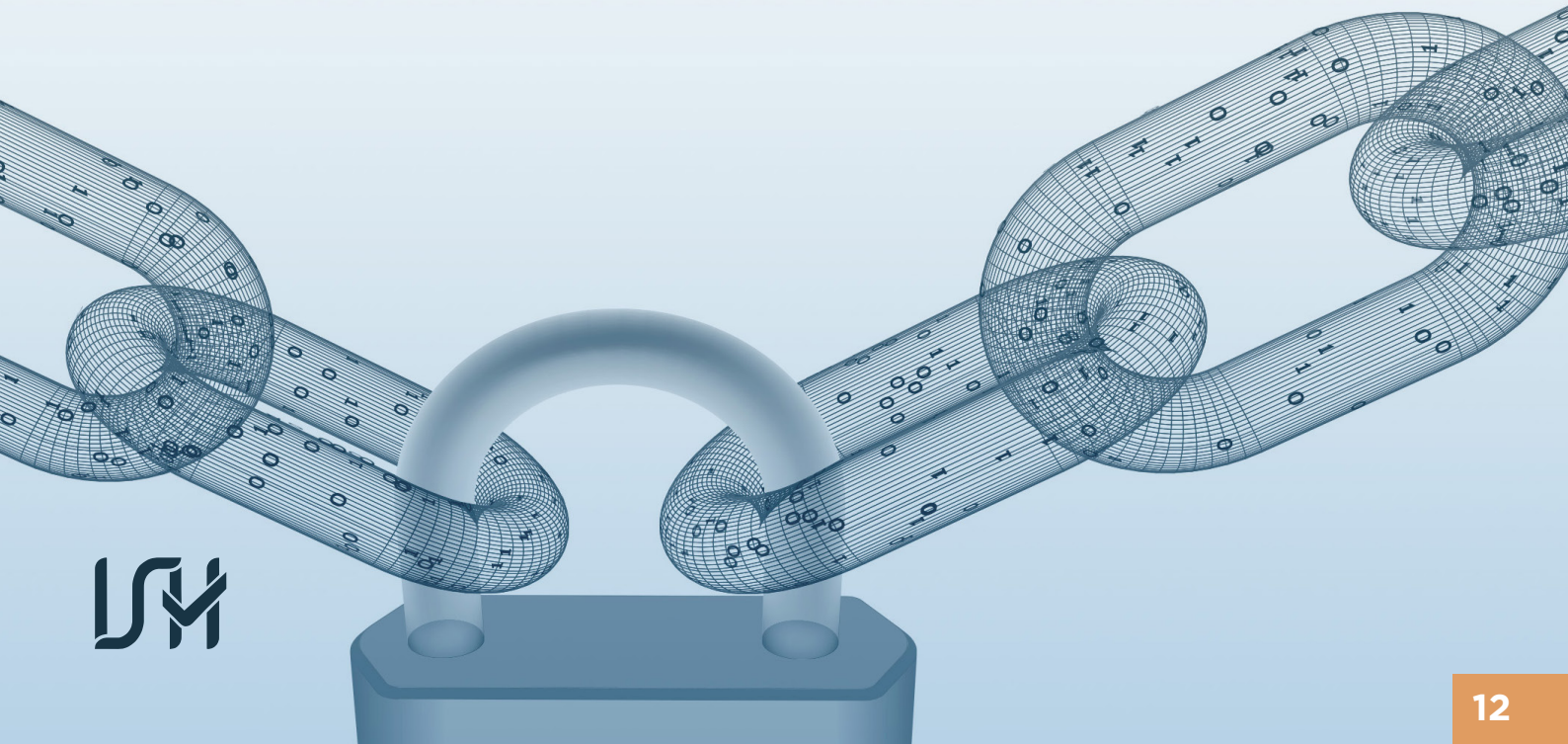
8 – SENHAS E AUTENTICAÇÃO MULTIFATOR

A maioria das empresas e usuários **armazena seus dados confidenciais online**, incluindo senhas de aplicativos e informações sobre serviços. Embora a senha seja um componente básico em segurança da informação, ela também **é uma das principais vulnerabilidades.** Qualquer violação ou uso inadequado dessas informações pode causar inúmeros prejuízos para as organizações.

Uma forma de aumentar a segurança dos dados é através da **Autenticação Multifator (MFA), que atua como uma camada adicional de segurança** para prevenir que usuários não autorizados acessem essas contas mesmo que a senha tenha sido roubada.

Ela exige que os usuários utilizem **duas formas de autenticação** para acessar a rede corporativa remotamente. A primeira é a tradicional, com login e senha. Já a segunda pode variar, dependendo do tipo de acesso, como um token por SMS, um código por e-mail, biometria, entre outros recursos.

Dessa forma, a autenticação multifator ajuda a **prevenir acessos não autorizados** às contas, tornando mais difícil para os cibercriminosos obterem acesso a informações confidenciais.



9 - GERENCIAMENTO DE VULNERABILIDADES

É fundamental que as empresas tenham uma **compreensão clara do cenário de ameaças** para tomar decisões mais informadas sobre o gerenciamento de riscos. Através do gerenciamento de vulnerabilidades, como o **Threat Intelligence**, as empresas podem **identificar, avaliar e tratar possíveis vulnerabilidades e configurações incorretas de segurança** em seus sistemas, garantindo uma visão atualizada da segurança.

O gerenciamento de vulnerabilidades **é um processo contínuo**, pois novas vulnerabilidades podem ser descobertas a qualquer momento. Assim, a identificação de falhas em todos os sistemas, redes e aplicativos requer ferramentas específicas, como scanners.

Esses programas são projetados para analisar os sistemas digitais da empresa e descobrir possíveis pontos fracos que possam ser explorados por hackers. Dessa forma, a empresa pode **tomar medidas preventivas** para proteger seus sistemas contra ataques cibernéticos.

10 – PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Um plano de recuperação de desastres em TI tem como objetivo **restaurar, de forma muito ágil, os dados e processos perdidos**. Dessa forma, no caso de acontecer uma falha, as operações e processos da empresa são facilmente estabilizadas.

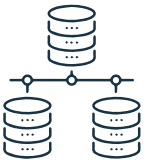
Para que isso seja possível, o plano deve ser **bem documentado, testado, avaliado periodicamente e melhorado ao longo do tempo**, buscando fazer uso das melhores práticas nesta disciplina.

Uma **pesquisa** aponta que **52% das empresas brasileiras** possui um plano de recuperação de desastres consolidado, no entanto, eles não foram atualizados recentemente.

Desenvolva um plano de recuperação de desastres que **amplie a sua capacidade de resiliência e recuperação cibernética**. É preciso descrever os procedimentos para a identificação, tomada de decisão e ações a serem executadas, de forma a minimizar perdas e garantir a continuidade das funções tecnológicas críticas do negócio após um desastre.

Além disso, existem dois conceitos importantes que devem ser definidos no PRD:

RTO (Recovery Time Objetive): é a meta que a organização define para o tempo máximo que a empresa deve levar para restaurar as operações normais após uma interrupção ou perda de dados.



RPO (Recovery Point Objetive): é a meta para a quantidade máxima de dados que a organização tolera perder.

Ação extra:

A integração de **GRC e IRM** na recuperação de desastres é essencial para garantir que as organizações possam lidar com incidentes de segurança da informação de forma eficaz.

O **Gerenciamento de Riscos de Informação (IRM)** permite que as organizações **identifiquem e avaliem os riscos** de segurança da informação que podem resultar em desastres, como ataques cibernéticos, falhas de sistema ou desastres naturais.

Enquanto, a **Governança, Risco e Conformidade (GRC)** ajuda as organizações a cumprir as regulamentações aplicáveis e a estabelecer políticas e procedimentos para lidar com incidentes de segurança da informação.

SAIBA MAIS AQUI

Ao integrar GRC e IRM da ISH na recuperação de desastres, as organizações podem se **preparar melhor para lidar com incidentes**, reduzir o tempo de inatividade, minimizando assim o impacto e garantindo a continuidade dos negócios.

A ISH PODE AJUDAR A IMPLEMENTAR A MELHOR ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA PARA A SUA EMPRESA

Entre em contato com nosso time de especialistas e conheça as melhores soluções de cibersegurança do mercado.