Cyber Security na Prática: por onde começar

ECOTRUST

A **Cyber Security** é um assunto muito discutido na atualidade e compõe a lista de prioridades dos gestores de empresas dos mais diversos portes e segmentos. Porém, para que ela seja efetiva e não apenas mais um protocolo a ser seguido, é preciso abordar o tema a partir de um ponto de vista mais prático.

“Cyber Security começa com a capacidade de reconhecer seu risco”

Nesse sentido, o primeiro passo para promover uma boa gestão de Cyber Security é **reconhecer os riscos cibernéticos** aos quais a sua empresa está exposta. Não há como pular esta etapa se você quer lidar eficientemente com os riscos e alcançar a resiliência cibernética.

A necessidade de compreensão dos riscos pode parecer óbvia, mas muitos gestores não dão a devida atenção a eles, embora adotem, em maior ou menor grau, algum protocolo de Cyber Security. O problema é justamente a transformação desse tipo de protocolo em algo burocrático, em um processo que é cumprido sem a devida reflexão sobre sua função prática. Este é o primeiro passo para uma gestão ineficiente de segurança cibernética.

O cibercrime tem se expandido de forma vertiginosa, em especial após a pandemia da Covid-19, e não existe um segmento de negócios que possa ser considerado livre desse tipo de ameaça. Ou seja, não há argumento para que você considere os riscos cibernéticos improváveis e cumpra o protocolo de Cyber Security apenas para garantir o mínimo nível de cuidado.

Enquanto os gestores negligenciam os riscos corridos, os cibercriminosos atuam de forma mais frequente, elaborada e complexa, representando uma grande ameaça para todas as empresas, independentemente de seu porte. Então cabe questionar:

Como você vai reagir ao se ver vítima de uma violação?

O que seria dito aos seus clientes e colaboradores?

Sua empresa seria capaz de lidar com os impactos negativos relacionados às finanças e à credibilidade?

Ela estaria preparada para enfrentar ações judiciais relacionadas ao vazamento de informações sensíveis?

Não basta, por exemplo, armazenar tudo na nuvem, pois lá também há grandes riscos cibernéticos. Você precisa **conhecer a fundo o seu ecossistema** e desenvolver um planejamento de Cyber Security eficiente e voltado para as especificidades do seu negócio, tendo sempre em mente que o aprimoramento deve ser constante, ou seja, sempre há algo para melhorar.

Ao longo deste e-book, você vai conhecer as etapas fundamentais para ter uma concepção mais pragmática da Cyber Security, além de contar com nossas sugestões para o seu gerenciamento e a sua resposta aos riscos detectados.

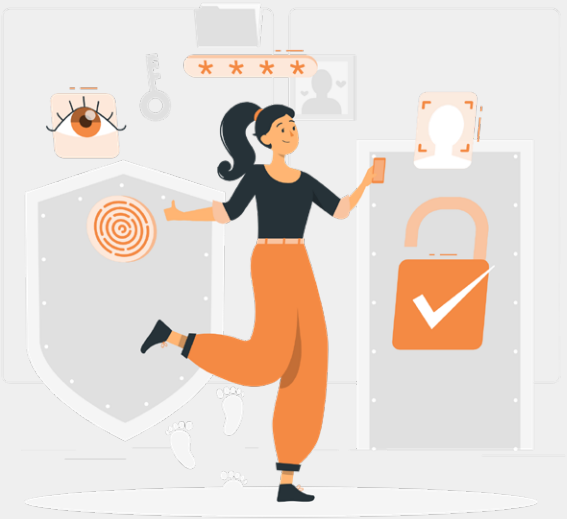
Sumário

1

Foco nos riscos e na resiliência

Muitos gestores ainda acreditam que basta contar com tecnologias avançadas na área de segurança para ter um bom programa de Cyber Security. A verdade é que não basta.
É óbvio que a tecnologia é fundamental, mas sozinha ela não resolve o problema. Você precisa **focar nos riscos e na resiliência associados à tecnologia** para obter bons resultados e manter seu negócio seguro.

Pode ser fácil implementar uma tecnologia de segurança e acreditar que você reduziu drasticamente todos os riscos corridos pelo seu negócio. Mas, infelizmente, esse investimento em tecnologia não traz nenhuma garantia de proteção contra as ameaças mais recentes e elaboradas. Assim, a sua abordagem de segurança precisa contar com a tecnologia, mas deve ser baseada nos riscos.



Em outros termos, os gestores ou líderes de um negócio precisam ter prática na identificação dos riscos e manterem-se concentrados em elementos específicos relacionados a esses riscos cibernéticos para diminuir o risco corporativo.

Os múltiplos componentes dos riscos cibernéticos precisam ser compreendidos e priorizados para que os **esforços de Cyber Security** da empresa sejam **direcionados para as áreas que mais necessitam**.

Somente assim uma empresa consegue ganhar resiliência cibernética e manter a Cyber Security sempre em dia com uma gestão de riscos eficiente. Nesse contexto, você pode seguir três recomendações práticas:

- **Entenda quais são e como se constituem as ameaças**

- **Meça o potencial impacto financeiro de uma exposição cibernética e o compare com os níveis de riscos que sua empresa está disposta e preparada para enfrentar**

- **Gerencie os riscos cibernéticos de maneira proativa, criando planos de ação claros baseados em suas capacidades de se proteger contra os crimes cibernéticos**

2

Abordagem baseada em **riscos**

Para criar uma resiliência cibernética que consiga lidar com novas e diferentes investidas dos cibercriminosos, a sua **abordagem precisa se basear nos riscos**. Isso vai permitir que a organização priorize os investimentos que incluam a solução de problemas relacionados às implementações baseadas na eficácia e no potencial de um programa cibernético para a redução de riscos específicos.

Esse programa deve atender às **metas de redução de riscos estabelecidas pelos gestores** e contar com uma implementação pragmática que alinhe os gestores e executivos com a equipe da linha de frente.

A abordagem baseada em riscos pressupõe que a empresa não vai buscar um controle sobre todas as áreas e setores que podem vir a ser o foco de um cibercrime. Ao invés disso, o foco estará na **construção de controles adequados para mitigar as piores vulnerabilidades**, criando a capacidade de derrotar as ameaças mais significativas que representam um alerta para as áreas críticas do empreendimento.

Ou seja, a abordagem baseada em risco para a segurança cibernética diz respeito a uma análise interativa que perpassa o negócio e também a uma ferramenta dinâmica que apoia a tomada de decisões estratégicas.

A Cyber Security deve estar focada no valor do negócio, utilizando uma linguagem comum entre as partes interessadas e **vinculando diretamente os riscos corporativos aos controles**. Assim, ela vai ajudar a traduzir as decisões executivas sobre redução de riscos e implementação de controles. O poder da abordagem baseada em risco para otimizar a redução de risco em qualquer nível de investimento é aprimorado por sua flexibilidade, ajustando-se a uma estratégia de análise dos riscos em evolução, conforme a necessidade.

Esse tipo de abordagem implica no reconhecimento de que **soluções de segurança perfeitas não existem**, mas, por outro lado, as empresas que conseguem, a partir dessa perspectiva, equilibrar de forma estratégica a segurança, a escalabilidade, o acesso, a usabilidade e o custo, conseguem proteger-se melhor a longo prazo contra os cibercriminosos, adversários que estão sempre em evolução.

Podemos dizer que a abordagem baseada em riscos é uma estratégia de segurança que atua de dentro para fora na empresa: enquanto outras concepções se focam nas ameaças e nas regulamentações externas, a abordagem proposta aqui é **direcionada para os riscos específicos do negócio**, que ditam a melhor estratégia de segurança e o direcionamento dos investimentos.

3

Identificação dos **cinco principais** riscos com base na prioridade

Uma forma de tornar a abordagem de Cyber Security baseada em riscos mais palpável é conhecer e listar os **cinco riscos de segurança prioritários do seu negócio**.

Ao defini-los, você deve conseguir responder a algumas questões como:

Qual seria o real impacto em termos de negócios de cada um dos cinco riscos?

Como esses impactos se alinham à quantidade de risco que sua empresa consegue assumir?

Você está realmente focado em apontar os riscos cibernéticos do seu negócio ou é orientado pela conformidade?

Como você pretende lidar com os riscos atuais e futuros? Qual é o seu planejamento para tratar esses riscos de maneira contínua?

Quando se pensa em governança e risco, há uma máxima de que **tudo o que é mensurável pode ser gerenciado**. Mas o foco na compliance tem sido o verdadeiro impulso na maioria das organizações, que destinam os principais recursos e investimentos de Cyber Security para a conformidade. Assim, muitas avaliações de risco são realizadas com uma abordagem de lista de verificação.

É claro que a conformidade é importante, mas o seu planejamento de Cyber Security precisa ser mais estratégico, compreendendo estruturas adequadas de gerenciamento de risco cibernético.

4

Equilíbrio entre riscos e **recompensas**

A chave para ter uma boa estratégia de Cyber Security é equilibrar riscos e recompensas, tomando **decisões assertivas de gerenciamento de riscos** alinhadas com os objetivos da sua empresa, sobretudo os objetivos de negócio.

Nesse sentido, você precisa atribuir responsabilidades de gerenciamento de riscos, estabelecer qual é a tolerância ao risco com a qual o seu negócio conta, adotar uma metodologia padronizada para avaliar os riscos e para responder de acordo com seus diferentes níveis, além de monitorar o risco de forma contínua.

5

Compreensão das estruturas de gerenciamento de **risco cibernético**

Além de compreender as especificidades dos riscos de segurança da sua empresa, é preciso explorar também as estruturas de gerenciamento destes riscos. Elas contam com uma **metodologia padronizada e documentada** para atividades como:

- **A realização de avaliações de risco que analisam as prioridades de negócios e identificam lacunas nos controles de segurança cibernética**

- **A realização de análise de riscos em lacunas de controle existentes**

- **A priorização do investimento futuro em segurança cibernética com base na análise de risco**

- **A execução da nova estratégia, implementando uma variedade de controles de segurança e práticas recomendadas**

- **A mensuração e pontuação da maturidade do programa de segurança cibernética ao longo do caminho**

6

Sobre as **avaliações** de riscos

Ao observar a lista acima, você deve ter se perguntado, o que vem a ser uma avaliação de risco. Em termos práticos, essas avaliações são definidas pelo NIST como avaliações usadas para identificar, estimar e priorizar riscos resultantes da operação e uso de sistemas de informação para as operações organizacionais, ativos, indivíduos, outras organizações e toda a sociedade em que o negócio se insere.

O objetivo principal de uma avaliação de risco cibernético é **manter as partes interessadas informadas e apoiar as respostas adequadas aos riscos identificados**. Elas também fornecem um resumo executivo para ajudar os gestores e diretores a tomarem decisões assertivas sobre segurança.

Mesmo que a relevância das avaliações de riscos cibernéticos seja evidente, muitas empresas optam por não realizá-las por conta da **complexidade percebida**. Muitos gestores preferem utilizar controles de segurança padronizados como respostas aos riscos sobre os quais eles ouviram falar. Com isso, as empresas acabam sendo detentoras de **programas de segurança desequilibrados**, sem adequação às suas especificidades e com foco nas prioridades erradas.

Os padrões e estruturas para as avaliações de riscos cibernéticos podem ser volumosos, mas são extremamente benéficos quando tomados como diretrizes para a formação de um ponto de partida simples.

Você pode criar uma **abordagem viável baseada em sua estrutura, cultura e perfil de risco**. O NIST 800-30, por exemplo, conta com modelos simples de avaliação de riscos, que podem ser utilizados independentemente da estrutura adotada.

Nesse contexto, existem algumas táticas recomendadas como foco para o seu gerenciamento de riscos e resiliência. Falaremos sobre elas nos tópicos seguintes.

7

Táticas para o gerenciamento de **riscos e resiliência**

Vamos ver agora algumas práticas que vão te ajudar a focar o seu programa de Cyber Security nos riscos e na resiliência.

Inventário de ativos

Para ter uma estratégia eficaz de proteção, é preciso **entender o que você está protegendo**. Só assim você vai conseguir tomar decisões estratégicas sobre Cyber Security e construir um bom plano de respostas a incidentes.

Ou seja, é fundamental conhecer os seus ativos de TI e saber qual é a importância de cada um deles para a sua empresa. Para cumprir essa missão de maneira assertiva e organizada, você precisa de um **inventário completo e detalhado dos seus ativos**, que seja gerenciado e **constantemente atualizado**. Sem esse inventário, você corre o risco, por exemplo, de não saber o que está conectado à sua rede.

A capacidade de rastrear e auditar seu inventário é um requisito básico para a maioria dos padrões de segurança, como o CIS Top 20, HIPAA e PCI. Todas essas normas possuem um elemento de avaliação de risco exigido das organizações. E se você realizar uma avaliação de risco documentada, precisará entender suas ameaças, vulnerabilidades e ativos.

Política de segurança da informação

Uma política de segurança da informação, não precisa ser implementada já como um documento extremamente complexo. Você pode **começar escrevendo o que já foi implementado em seu ambiente de TI**.

O importante a princípio é documentar as práticas que já estão sendo adotadas. Na medida em que o seu programa de Cyber Security for adquirindo novas nuances, **a sua política de segurança deverá ser atualizada**. Se, quando comparada com um padrão alvo, a prática não atender ao padrão, ela pode ser modificada tanto na política escrita quanto na implementada.

Para ser considerada eficaz, uma política de segurança da informação precisa manter o foco nos objetivos e estratégias de negócios, cobrir processos de segurança de ponta a ponta em toda a empresa, incluir atualizações e monitoramentos contínuos e promover a responsabilização e a aplicação nas rotinas da empresa.

Priorização na correção de vulnerabilidades

Sua empresa não conseguirá corrigir todas as vulnerabilidades de segurança simultaneamente por várias razões. Por exemplo, você pode contar com uma limitação de recursos.

Assim, é imprescindível o **discernimento entre as vulnerabilidades críticas e as não críticas**. As equipes de segurança da informação devem conseguir fazer essa delimitação e tomar decisões pragmáticas para tornar as vulnerabilidades gerenciáveis.

Para isso, você precisa recorrer a fontes de inteligência externas e internas, como a importância comercial, a postura de segurança, os registros de riscos, os sistemas de gerenciamento de mudanças e os dados de pentest.

Também recomendamos que você utilize **ferramentas VPT**, que são tecnologias avançadas dedicadas à priorização de vulnerabilidades a partir da identificação e avaliação das mesmas de forma mais proativa.

Plano de resposta a incidentes

É preciso saber **o que fazer e por onde começar** no caso de um incidente de segurança. Nesse sentido, você deve construir o seu plano de resposta a incidentes, que precisa **identificar as pessoas responsáveis por invocar o plano e liderar as respostas**, além de traçar funções e responsabilidades claras para todos os componentes da equipe de resposta.

Com o seu plano elaborado, os exercícios de mesa podem cristalizar as respectivas **funções dos integrantes da equipe**, aprimorar as habilidades necessárias para lidar com um incidente e facilitar o trabalho em equipe após o mesmo.

Construa um plano rigoroso de backup e recuperação de desastres que seja testado e atualizado regularmente. Isso será fundamental, dada a maior ameaça de ataques de ransomware.

O objetivo da gestão de incidentes **é identificar e responder a qualquer evento imprevisto** e perturbador e limitar seu impacto em um negócio. Esses eventos podem ser técnicos — como a negação de serviço (DoS), malware ou intrusão de sistema — ou podem resultar de um acidente, um erro ou uma falha de sistema ou processo.

A diferença entre uma mera inconveniência e uma catástrofe total para sua organização pode vir de sua capacidade de detectar e avaliar o evento, identificar sua origem e causa e ter soluções prontamente disponíveis. Portanto, crie um plano robusto de resposta a incidentes.

8

Conclusão

Você não vai conseguir eliminar todos os riscos de segurança da sua empresa. Os seus recursos contam com limites e as ameaças são numerosas e diversificadas. O que você tem a fazer é **reduzir os riscos a um nível aceitável a partir de controles efetivos de segurança e privacidade**.

Porém, é preciso ter em mente que esses controles vão se tornar inadequados futuramente. Daí a importância de tornar a estratégia de Cyber Security **um processo em constante aprimoramento**.

Diferentes tipos de riscos pressupõem diferentes estratégias de defesa e as medidas defensivas precisam ter custos proporcionais ao dano potencial de uma violação de dados e à probabilidade de ocorrência dessa violação.

A **gestão de riscos da Cyber Security** está em um ponto de importante evolução. Ela já é reconhecida como fundamental até mesmo para a estabilidade financeira de uma organização e também para a conformidade regulatória. Porém, o maior desafio é a definição das melhores medidas de segurança, uma vez que cada empresa tem objetivos, requisitos e tolerâncias a riscos diferentes.

Nesse sentido, você deve avaliar cautelosamente o patamar em que estão hoje e as condições que deseja atingir futuramente em termos de Cyber Security. Assim, é possível **construir um roteiro de redução dos riscos** à medida em que os negócios se expandem.

Eco Trust

Adotar métodos corretos e eficientes e aplicá-los com regularidade pode resultar na **economia de custos e aumento da competitividade** de negócios que dependem de tecnologia. As vantagens da segurança da informação e da proteção de dados para o presente e o futuro são diversas e podem evitar prejuízos muito severos.

É importante entender que processos relacionados a gestão de vulnerabilidades são os verdadeiros **investimentos em prevenção** e cuidados mais do que necessários. É hora de começar a agir de forma eficiente o mais rápido possível em favor da continuidade do negócio. Veja como a Eco IT pode te ajudar.

A **EcoTrust**, nossa **plataforma de *Inteligência em Riscos Cibernéticos***, possibilita que os líderes de Segurança e TI possam tomar decisões importantes de forma mais assertiva quando o assunto for segurança cibernética. Através da descoberta e gerenciamento de vulnerabilidades e riscos cibernéticos, de forma orquestrada, simplificada e com abordagem orientada aos riscos de negócio, a plataforma traz uma visão estratégica (negócio) com embasamento em indicadores técnicos (táticos e operacionais).

E para comprovar todas essas vantagens, você pode experimentar a plataforma gratuitamente. Basta clicar no botão abaixo.

Conhecer a solução

Entre em contato

site

www.ecotrust.io

ECOTRUST