Defcon 1
Information Technology

Symantec.
by Broadcom Software

Estratégia DLP:
7 erros mais comuns
e como evitá-los

Guia Rápido

Uma boa estratégia de DLP precisa atender pontos essenciais para garantir a sinergia do seu ecossistema, equilibrando dados sigilosos, governança do negócio, gerenciamento de políticas e o uso de ferramentas adequadas.

Se você está iniciando a sua estratégia ou pretende fortalecê-la, confira esses 7 erros mais comuns em Segurança da Informação e saiba como evitá-los para ter sucesso na sua jornada de proteção.

Erro #1

Não envolver os líderes de negócios

O profissional responsável pela estratégia de DLP, naturalmente, pode não conhecer a rotina e as necessidades técnicas de todas as áreas do negócio.

O contrato da área de vendas é sigiloso ou não?
Quem tem acesso aos arquivos do RH?

Para responder todas as perguntas e desenhar uma estratégia poderosa, o primeiro passo é realizar conversas e entrevistas com os líderes de negócio para entender cada realidade. Ganhando conhecimento de quais dados são sensíveis, como são gerados, o seu ciclo de vida e qual o tipo de proteção necessária para cada um.

Entrevistando os líderes de negócio, você vai entender todos os processos e os fluxos dos dados dentro da organização e, a partir disso, vai estar preparado para escrever uma política sob medida, que as pessoas consigam cumprir.

Erro #2

Escrever uma política inadequada

A etapa de conversar com os líderes vai ajudar a mitigar a chance de escrever uma política não aderente à organização, afinal, você já vai ter entendido as necessidades reais das áreas de negócio.

Mas, ainda assim, você pode cometer erros na hora de escrever uma política, seja por ser simples demais, deixando de proteger os dados, ou muito restritiva, impedindo o negócio de funcionar de forma ágil e abrindo brechas para o seu descumprimento.

É necessário escrever uma política que permita equilibrar os riscos e as necessidades do negócio e, claro: que seja simples de aplicar, entender e cumprir no dia a dia.

Erro #3

Não ter uma estrutura de monitoramento

Você realizou a entrevista, mapeou as necessidades e já escreveu uma política que cumpre com os requisitos de negócio: perfeito! Mas ainda não acabou.

Na maioria das vezes, as políticas vão precisar de ajustes mesmo depois de lançadas, porque é normal que alguns pontos não tenham sido mapeados desde o início, seja por não ter estruturado Casos de Uso ou simplesmente porque o negócio mudou.

Por isso, ter uma estrutura para monitorar continuamente, fazer a observabilidade da política e revisá-las quando necessário é essencial para entender o que está funcionando ou não, e evoluir constantemente na proteção.

Erro #4

Não criar gatilhos para compliance e alterações da política

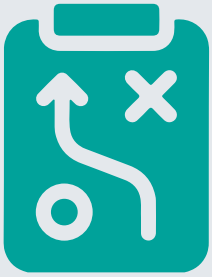
Você precisa entender que todo esse processo é dinâmico e que as mudanças fazem parte, por isso, é necessário criar gatilhos que preveem as necessidades de alterações da política.

A lei que rege o meu negócio mudou e agora?
Entrou um novo colaborador na empresa, como fazer?

O ideal é estabelecer o processo de compliance contínuo para as mudanças, englobando gatilhos e uma estrutura que permita alertar quando existir a necessidade de alteração de uma política.

Erro #5

Não seguir um plano de comunicação



Não esqueça do plano de comunicação, seja para comunicar a implementação da política ou para reportar incidentes.

Como eu comunico o problema?
Para quem eu comunico?
Como será o fluxo de comunicação?

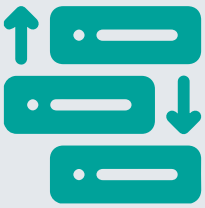
A comunicação vai definir os papéis e as responsabilidades de todos os envolvidos e mantê-los informados e sensibilizados sobre a importância dos dados, os riscos e os impactos em caso de descumprimento da política.

É essencial comunicar e educar todos os colaboradores, deixando claro que eles estão lidando com dados que podem ser sigilosos e de extrema importância para o funcionamento do negócio. Essa atitude fortalece as equipes e a cultura da empresa em relação à proteção de dados.

Não esqueça: uma boa comunicação pode ser a chave para a redução de incidentes.

Erro #6

Não analisar nem responder o volume de incidentes



Se você conseguiu evitar todos os erros anteriores, esse erro de gestão de incidentes você vai tirar de letra!

Vamos imaginar que todos os dias surgem mil incidentes. Dificilmente você terá uma estrutura para analisar todos eles ao mesmo tempo e é por isso que é essencial estabelecer os critérios de priorização.

Assim, você consegue filtrar e classificar os incidentes, ajudando a definir qual deles é mais crítico para você tratar primeiro.

E, claro, tão importante quanto filtrar os incidentes, o administrador de DLP precisa conseguir evitá-los. E isso é possível utilizando uma ferramenta madura e eficaz. Afinal, uma grande parte dos incidentes reportados são conhecidos como falsos positivos e, com a ajuda da ferramenta certa, é possível criar exceções para que esse tipo de incidente pare de ser gerado, diminuindo significativamente o número e ajudando a equipe a se concentrar no que realmente importa.

Erro #7

Contar com uma ferramenta de DLP que não protege todos os perímetros da empresa

Esse último erro é mais comum do que você imagina e pode ajudar a evitar ou potencializar os outros erros na sua estratégia de DLP.

A sua ferramenta protege todos os perímetros da empresa?
Ela dá conta de integrar todos os alertas?
É simplificada e unificada com outras soluções?

A escolha da ferramenta é decisiva para o sucesso. Por isso, contrate uma ferramenta ilimitada e completa, que garante a proteção de endpoint, e-mails, rede, nuvem e todos os perímetros da empresa, possibilitando um plano de segurança realmente eficiente.

Com **Defcon1 e Symantec** você **evita todos os erros** e conquista uma proteção de dados de ponta a ponta

A Defcon1 combina serviços exclusivos de consultoria e de suporte para todas as áreas da cibersegurança com as mais avançadas soluções Symantec, garantindo proteção para endpoint, rede, e-mail e nuvem.

Defcon1 é
PREMIER PARTNER
Symantec. by Broadcom Software
BRASIL

São anos de experiência em transformar regras de negócios em políticas de proteção de dados

Com a consultoria de Defcon1 é possível desenhar uma estratégia de DLP poderosa e identificar com agilidade as necessidades do negócio, fortalecendo a construção, comunicação e gerenciamento das políticas de segurança.

Defcon 1
Information Technology

Symantec
by Broadcom Software

Conte com a gente!

Estamos preparados para te ajudar com a melhor estratégia de DLP.

Principais certificações técnicas em cibersegurança

Experiência e credibilidade em aplicação de soluções

Foco em solucionar desafios técnicos com agilidade e eficiência

55 (11) 3280-8669

Al. santos 1773, sala 610, 6 Andar | São Paulo - SP

@comercial@defcon1.com.br