CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Manual de procedimentos de prontidão cibernética

Um guia prático para ajudar a reduzir o risco cibernético e a defender contra os problemas cibernéticos mais comuns.

Este manual de procedimentos faz parte do Programa de prontidão cibernética do Cyber Readiness Institute e baseia-se nas melhores práticas dos principais especialistas em cibersegurança.

Uma mensagem para o Líder cibernético:

Em primeiro lugar, gostaríamos de agradecer-lhe por dedicar tempo a concluir o Programa de prontidão cibernética. É um exercício importante que irá ajudar a sua organização a tornar-se mais resiliente face aos problemas cibernéticos mais comuns, e você, enquanto Líder cibernético, desempenha um papel fundamental neste processo.

Chegou agora o momento de usar o que aprendeu nas primeiras fases do programa e implementar alterações significativas na sua organização através de políticas e planos internos. No Manual de procedimentos de prontidão cibernética, incluímos orientações políticas bem definidas e passíveis de serem colocadas em prática para cada um dos problemas cibernéticos principais. O documento contém campos em branco para preencher, onde poderá introduzir o nome e as informações da sua organização, bem como personalizar estas políticas no documento, bem como uma lista de verificação que o vai ajudar a monitorizar o seu progresso. Também poderá incorporar o texto nos seus documentos internos e personalizar o conteúdo à medida das necessidades únicas da sua organização.

O programa pode ser utilizado de duas formas para melhorar a prontidão cibernética da sua organização. A primeira abordagem é fazer o programa online e partilhar o que aprendeu com a sua organização. Se decidir dar o próximo passo, a segunda abordagem exige que um Formador de cibersegurança do CRI analise o seu Manual de procedimentos para verificar se implementou os requisitos do CRI.

> **1) Auto-conclusão + Receção do certificado de conclusão:** Conclua este programa online e utilize o Manual de procedimentos para adotar as políticas chave e desenvolver um plano de continuidade da atividade.
> **2) Conclusão verificada + Receber a certificação de prontidão cibernética do CRI:** Conclua este programa online, utilize o Manual de procedimentos para adotar as políticas chave e desenvolver um plano de continuidade da atividade, dar formação à sua força de trabalho e enviar um certificado assinado, bem como ter o seu Manual de procedimentos completo analisado e verificado por um Formador de cibersegurança do CRI.

Além disso, o Manual de procedimentos inclui diretrizes para um Plano de continuidade da atividade. Mesmo com a melhor higiene cibernética, os sistemas podem ser comprometidos. Quando isso acontece, é importante dispor de um plano de ação bem definido para mitigar o impacto. Convida-mo-lo a copiar o Plano de resposta a incidentes e integrá-lo nas suas políticas internas. Depois de o fazer, irá dispor de um enquadramento que pode ser convertido em ação, se necessário.

Obrigado novamente por participado no Programa de prontidão cibernética. Desejamos-lhe a si e à sua organização o maio dos sucessos.

Acerca do programa

O programa de prontidão cibernética é uma forma simples e prática de as organizações oferecerem formação em sensibilização para a segurança aos funcionários e estabelecerem práticas de prontidão cibernética sustentáveis e eficazes. Concebido especificamente para pequenas e médias empresas, este programa centra-se no comportamento humano e irá ajudá-lo a criar colaboradores capacitados, formados e envolvidos em práticas de higiene cibernética eficazes que têm um efeito direto na segurança e na viabilidade da sua empresa.

Saiba mais em: cyberreadinessinstitute.org

Índice

Visão geral do programa de prontidão cibernética

Abordar a causa original dos problemas de cibersegurança

Com o nosso mundo cada vez mais interligado, as empresas enfrentam desafios cada vez mais complexos para proteger as suas informações e tecnologias, o que torna a prontidão cibernética mais fundamental do que nunca. Os ciberagentes maliciosos exploram os hábitos comuns e os comportamentos previsíveis para contornarem inclusivamente as tecnologias de segurança mais avançadas. Por isso, o Cyber Readiness Institute desenvolveu um programa de formação focado especificamente no comportamento humano.

O Programa de prontidão cibernética é uma forma simples e prática de a sua organização aumentar a sensibilização e estabelecer práticas de prontidão cibernética sustentáveis e eficazes. O Programa foi concebido especificamente para as pequenas e médias empresas, com um foco no comportamento humano para ajudá-lo a criar uma força de trabalho capacitada, formada e envolvida em práticas de higiene cibernética eficazes que têm um impacto direto na segurança e na viabilidade da sua empresa.

Programa gratuito

O Programa é gratuito e requer conhecimentos técnicos mínimos para ser concluído. Desde modelos de políticas a materiais de formação, oferecemos tudo o que precisa para desenvolver as suas competências cibernéticas e envolver a sua força de trabalho para criar uma organização preparada para a cibernética.

Função de Líder cibernético

Como Líder cibernético, o seu papel é influenciar positivamente o comportamento humano, sensibilizar e obter o compromisso da força de trabalho, bem como envolver a alta direção para criar uma cultura de prontidão cibernética de cima para baixo na sua organização.

Para ser Líder cibernético eficaz, é necessário ter fortes competências de gestão e de recursos humanos, dominar a tecnologia, ter capacidade para desempenhar a função, ter uma paixão pela importância da cibersegurança e contar com o apoio da direção.

Os Líderes cibernéticos compreendem que a prontidão cibernética não é mais uma caixa a preencher, mas sim uma prática e um hábito contínuos em que os colaboradores podem ver o valor e o panorama geral, apreciar o impacto que têm na segurança enquanto indivíduos, compreender as aplicações de segurança pessoal e sentir-se capacitado para fazer perguntas e alterar comportamentos regularmente.

Como Líder cibernético designado, irá receber formação sobre os princípios básicos da prontidão cibernética, desenvolver políticas e procedimentos cibernéticos para a sua empresa e, em seguida, formar os colaboradores da sua empresa para obter uma Certificação de prontidão cibernética.

Se só pretende obter um Certificado de conclusão, poderá concluir o Programa e o Manual de procedimentos ao seu próprio ritmo, sem ter de enviar um Manual de procedimentos para obter certificação.

Se pretende obter a certificação de Prontidão cibernética, utilize a seguinte lista de verificação enquanto avança no Manual de procedimentos para assegurar que cumpriu todos os requisitos antes de os enviar para info@cyberreadinessinstitute.org.

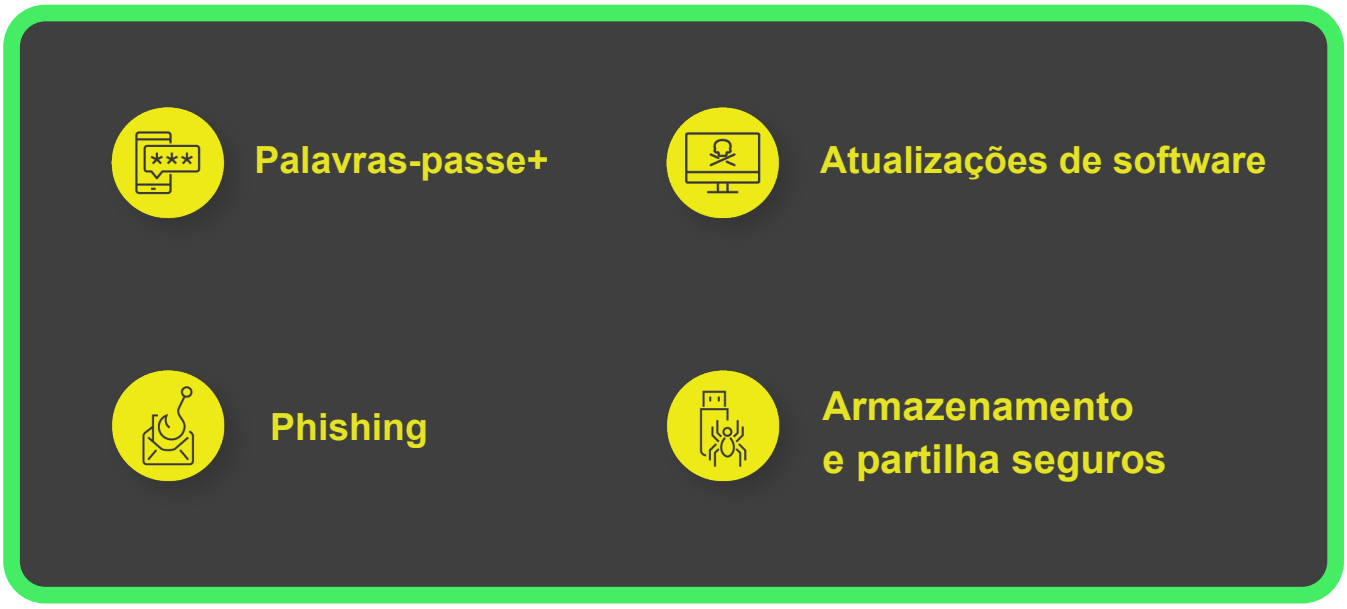
	Data de conclusão	Notas
Líder cibernético designado e informações de contacto documentadas		
Métrica de referência registada		
Políticas dos 4 principais problemas de cibersegurança estabelecidas		
Ferramenta de gestão de atualizações de software concluída		
Ficha de trabalho de definição de prioridades concluída		
Plano de resposta a incidentes concluído		
Formação da força de trabalho sobre os 4 principais problemas de cibersegurança e a continuidade da atividade concluída		
Documento de certificação de formação assinado		
Métricas de reavaliação registadas		
Programa online de prontidão cibernética concluído		
Manual de procedimentos enviado para análise (se pretende obter a Certificação)		

Políticas de 4 principais problemas de cibersegurança

O Programa de prontidão cibernética está focado em quatro políticas chave por serem tanto a causa da maioria dos problemas de cibersegurança como as mais fáceis de evitar. A forma como os colabores gerem as palavras-passe e a autenticação, as atualizações de software, a formação para a sensibilização para o phishing e os dados definem a postura de segurança de uma organização.

Estes requisitos de políticas são fáceis de implementar e gerir para organizações de todas as dimensões. Proporcionar um nível básico verificável das práticas e procedimentos de cibersegurança que todos na sua organização devem cumprir.

Estes requisitos devem ser aplicados a todos os colaboradores e contratantes que acedem aos sistemas e redes da empresa em todos os dispositivos, incluindo computadores, telemóveis e tablets. Isto aplica-se aos dispositivos fornecidos pela empresa e aos dispositivos pessoais.



Acerca das palavras-passe

A autenticação e as palavras-passe asseguram o acesso das pessoas certas aos sistemas, recursos e informações corretos de que precisam para realizar o seu trabalho todos os dias. Alguns componentes chave incluem palavras-passe, perguntas de segurança, autenticação multifator e informação biométrica (por exemplo, leitura de impressões digitais, reconhecimento facial). É provável que os colaboradores na sua organização utilizem muitos sistemas e dispositivos diferentes que requerem uma palavra-passe ou algum tipo de autenticação. Isto inclui credenciais de conta, acesso a bases de dados, início de sessão no seu computador, nomes de utilizadores, crachás e mais.

Palavras-passe+:

A primeira linha de defesa contra hackers oportunistas é a autenticação forte, que consiste em palavras-passe longas, e na utilização da autenticação multifator (MFA). A ativação da autenticação forte demora apenas alguns minutos e é uma parte essencial da boa higiene cibernética. Um compromisso organizacional para a utilização de práticas de autenticação fortes irá assegurar que só as pessoas certas têm acesso aos sistemas, recursos e informações certos.

Requisitos da política do CRI:

1. A MFA deve ser ativada em todo o hardware e software que a suporte.
2. As palavras-passe devem ter, pelo menos, 15 caracteres de comprimento. Se uma aplicação ou dispositivo não permitir 15 caracteres, as palavras-passe deverão ter o comprimento máximo permitido.
3. Não é necessário alterar periodicamente as palavras-passe. Se existirem provas de uma falha de cibersegurança, todas as palavras-passe devem ser alteradas imediatamente.

Acerca de atualizações de software

As correções de segurança nas atualizações são denominadas "patches." Estas correções preenchem lacunas de segurança representadas pelas vulnerabilidades identificadas que os hackers conseguem explorar. A vasta maioria dos ciberataques visa sistemas com vulnerabilidades reconhecidas e já corrigidas numa atualização de software que simplesmente não tinha sido instalada, podendo estes ataques ter sido prevenidos se as atualizações estivessem em vigor.

Atualizações de software:

A maioria dos ciberataques visa sistemas com vulnerabilidades conhecidas. A atualização regular do software assegura que as funcionalidades de segurança mais recentes estão a funcionar para si.

Requisitos da política do CRI:

1. Desenvolver um processo de atualização de software através da Ferramenta de gestão de atualizações de software do CRI

Acerca do phishing

Phishing é um ataque cibernético que utiliza e-mails e mensagens enganadores para obter acesso à rede de uma organização. O phishing visa indivíduos ao enganar o destinatário do e-mail ou da mensagem de texto, levando-o a clicar numa hiperligação ou a descarregar um anexo, o que pode resultar na infeção do dispositivo com malware ou em permitir que o hacker aceda aos sistemas ou contas de alguém. Estas mensagens costumam ser oportunistas, assumindo fraudulentamente a forma de comunicações reais que podemos receber legitimamente.

Phishing:

O phishing utiliza mensagens enganosas para obter acesso à rede e aos dados de uma organização. Qualquer pessoa com uma conta de e-mail ou um smartphone pode colocar a sua organização em risco ao clicar em ligações em mensagens de phishing. Para diminuir o risco de uma tentativa de phishing bem-sucedida, os colaboradores devem fazer regularmente uma formação de sensibilização adequada para se manterem atualizados sobre a natureza evolutiva desta ameaça.

Requisitos da política do CRI:

1. As comunicações de sensibilização para o phishing enviadas mensalmente a todos os colaboradores.
2. Todos os colaboradores estão obrigados a concluir trimestralmente a formação em phishing, que deve incluir, no mínimo: sensibilização, exemplos e métodos de resposta.
3. Os novos colaboradores estão obrigados a concluir com êxito a formação em phishing como parte do seu processo de integração ou no prazo de 30 dias após a sua data de início.

Acerca do armazenamento e partilha seguros

A forma como armazena e partilha documentos e dados na rede informática da sua organização é uma parte essencial da sua preparação para cibernética. As cópias de segurança regulares e uma política de unidades USB sólida são essenciais para manter a sua organização segura e resiliente.

Armazenamento e partilha seguros:

As unidades USB e outras formas de suportes amovíveis são portadoras comuns de vírus e malware. A definição de políticas e orientações sólidas para unidades USB e suportes amovíveis ajudará a manter os dados seguros e a evitar os ataques desnecessários. Com o armazenamento na cloud, a sua organização poderá armazenar dados na Internet através de um fornecedor que gere e opera o armazenamento de dados como um serviço.

Requisitos da política do CRI:

1. Proíba a utilização de unidades USB e de dispositivos multimédia amovíveis, exceto em casos críticos pré-determinados para a empresa. (Consulte Sugestões, truques e orientação para ver exemplos.)
2. Dê prioridade ao armazenamento na cloud para a transferência e o armazenamento de ficheiros em todas as aplicações, quando disponível.
3. Ative a encriptação automática para a transferência e o armazenamento de ficheiros em todas as aplicações, quando disponível.
4. Devem ser feitas cópias de segurança periódicas de todos os dados críticos da empresa em suportes amovíveis seguros e fiáveis e/ou no armazenamento na cloud seguro e fiável.

Políticas cibernéticas de [a sua organização]

Instruções de utilização:

O seguinte modelo de política deve ser utilizado para desenvolver ou registar as políticas cibernéticas da sua organização.

Se a sua organização ainda não tiver políticas cibernéticas, pode simplesmente adicionar o seu logótipo ao modelo do CRI e utilizar as nossas políticas como se fossem suas.

Se a sua organização já tiver políticas cibernéticas que cumprem ou superam os requisitos do CRI, utilize o seguinte modelo para registar essas políticas para análise.

Palavras-passe:

Nome da política	Detalhes da política

Atualizações de software:

Nome da política	Detalhes da política

Phishing:

Nome da política	Detalhes da política

Partilha segura de ficheiros:

Nome da política	Detalhes da política

Ferramenta de gestão de atualizações de software

Instruções de utilização:

Esta ferramenta irá ajudá-lo a fazer o seguimento das atualizações de software necessárias para manter a sua organização a funcionar em segurança. Utilize esta ferramenta para indicar o software que a sua organização utiliza e que necessita da implementação de atualizações. Esta ferramenta não se destina a inventariar e a monitorizar as atualizações de software em dispositivos individuais, mas lembre-se de dar formação aos colaboradores sobre a importância de ativar a atualização automática. Pense nos diferentes tipos de software que utiliza, tais como: sistemas (Windows, MacOS), aplicações (Office 365, QuickBooks) e outros (Zoom, Anti-Virus).

1. Indique o software utilizado pela sua organização na Coluna A. Os exemplos listados na ficha de trabalho irão ajudá-lo a dar os primeiros passos. Adicione uma linha para qualquer software que utilize e que não conste na lista, e elimine uma linha para qualquer software que a sua empresa não utilize.

2. Determine quem é responsável pela atualização do software na Coluna B, por exemplo, o departamento de TI, o fornecedor, etc.

3. Indique quem utiliza o software (todos os colaboradores, marketing, vendas, contabilidade) na coluna C

4. Agora que tem esta lista, faça uma classificação rápida para identificar se o software tem prioridade alta, média ou baixa para o funcionamento da sua atividade principal. Consulte a Ficha de trabalho de definição de prioridades no seu Plano de continuidade da atividade para classificar a prioridade de cada software na Coluna D.

5. Utilize as informações das colunas B a D para determinar se a atualização automática deve ser ativada na coluna E. Em caso de dúvida, ative a atualização automática.

6. Se a atualização automática não estiver ativada, poderá utilizar esta ferramenta periodicamente para registar a data da última atualização concluída na coluna F.

Software	Quem é o responsável pela sua atualização?	Quem o utiliza?	Prioridade	Atualização automática ativada	Data de conclusão da última atualização
Apple iOS	Utilizador	Todos os colaboradores	Alta	Sim	
MacOS					
Microsoft Windows					
Office 365					
PayPal					
QuickBooks					
Slack					
Square					
Xero					
Zelle					
Zoom					

Plano de continuidade da atividade

Um plano de continuidade da atividade oferece a uma empresa a oportunidade de planear a sua capacidade de continuar a fornecer produtos e serviços em prazos aceitáveis, e com uma capacidade predefinida durante uma crise. O plano irá apoiar os objetivos estratégicos, proteger a reputação e a credibilidade, e permitir que se mantenha resiliente face a um ciberataque.

O desenvolvimento deste plano irá ajudá-lo a antecipar-se à ameaça. Acredite quando lhe dizermos que não querer saber como reagir durante um incidente. O tempo de resposta é fundamental para minimizar os danos.

Para desenvolver o seu Plano de continuidade da atividade, deve elaborar o seguinte:

1. Ficha de trabalho de definição de prioridades: uma ferramenta que lhe permite inventariar os dados e as informações mais importantes para o êxito da sua organização. A definição da prioridade do que é mais importante proteger irá ajudá-lo a criar políticas eficazes e a tomar decisões de investimento inteligentes.

2. Plano de resposta a incidentes: Um plano abrangente e gradual para responder, corrigir e aprender rapidamente com cada incidente.

A ferramenta de atualização de software e a política de cópia de segurança dos dados também são fatores chave que contribuem para a sua resiliência global.

Existem outros recursos incluídos mais adiante no Manual de procedimentos que o vão ajudar a reforçar a sua cibersegurança e resiliência, à medida que continua a melhorar o planeamento da continuidade da atividades da sua organização.

Ficha de trabalho de definição de prioridades

É chegado o momento de pensar nos dados, no software e no hardware mais importantes para o êxito da sua organização. A definição da prioridade do que é mais importante proteger irá ajudá-lo a criar políticas eficazes e a tomar decisões de investimento inteligentes.

Indique os dados mais importantes para o êxito da sua organização (números de cartões de crédito dos clientes, informações pessoais dos colaboradores, dados financeiros, etc.)

Indique o software mais importante para o êxito da sua organização (Office 365, MacOS, QuickBooks, etc.)

Indique as ferramentas de hardware e de software mais importantes para o funcionamento da sua organização (dispositivos móveis, portáteis, impressoras, scanners, etc.)

Identifique os 3 a 5 elementos das 3 listas precedentes que causariam mais danos à sua empresa se fossem perdidos, roubados ou não estivessem disponíveis.

Plano de resposta a incidentes (IRP)

Estabelecer práticas e políticas de prontidão cibernética ajuda a reduzir o risco, mas é importante assumir que a nossa empresa irá provavelmente enfrentar a qualquer momento um incidente de segurança que poderá ter impacto nas operações empresariais. Tentar determinar como responder durante um incidente não é boa ideia. O tempo de resposta é fundamental para minimizar os danos. Dispor de um plano bem definido pode fazer a diferença entre um incidente e uma catástrofe.

Um IRP abrangente e gradual permite responder, corrigir e aprender rapidamente com cada incidente. Este IRP funciona como um roteiro para o que fazer durante a resposta a um incidente de cibersegurança, o que assegura uma resposta estratégica e não apenas uma resposta reativa.

A nossa resposta a incidentes inclui três elementos principais:

1. **Preparar** para um possível incidente no futuro
2. **Responder** durante o incidente
3. **Recuperar** do incidente

Preparar

Diretrizes organizacionais:

O investimento que fizer na preparação trará muitos dividendos. Existem alguns elementos de resposta essenciais que devem ser realizados o mais brevemente possível para se preparar para os danos causados por um ataque e os reduzir. O CRI irá analisar e confirmar que incluiu o seguinte no seu Manual de procedimentos final.

1. **Nomear o líder de cibersegurança.** A nomeação de um líder de cibersegurança é essencial para a prontidão cibernética da sua empresa. O Líder de cibersegurança será responsável pela partilha de informações de prontidão cibernética com a sua força de trabalho e pela gestão do desenvolvimento das suas políticas de prontidão cibernética.

Medidas implementadas	Data de conclusão

2. **Implementar Políticas de 4 principais problemas de cibersegurança:** assegure que as políticas cibernéticas são definidas e partilhadas com os colaboradores que cumpram ou vão mais além dos requisitos do CRI.

Medidas implementadas	Data de conclusão

3. **Faça cópias de segurança dos dados e certifique-se de que consegue voltar a instalar os dados a partir das cópias de segurança.** A recuperação de um ataque será muito mais rápida e afetará muito menos as operações se tiver cópias de segurança atualizadas do software do sistema, das aplicações e, sobretudo, dos dados importantes. Também deverá assegurar que todas as pessoas na sua organização têm cópias de segurança, caso este processo não esteja centralizado. É importante testar regularmente as suas cópias de segurança.

Medidas implementadas	Data de conclusão

4. **Dê formação à sua força de trabalho.** Todos os membros da equipa devem conseguir identificar atividades suspeitas e saber quem contactar nesta eventualidade. Os colaboradores essenciais também deverão estar cientes do seu papel na resposta a um incidente.

Medidas implementadas	Data de conclusão

5. Estabelecer contactos. Estabeleça contactos internos e externos aos quais poderá recorrer se um incidente cibernético superar a sua capacidade de controlo.

Contacto para emergência de TI	[Indique aqui]
Fornecedor de serviços Internet	[Indique aqui]
Contacto para emergência jurídica	[Indique aqui]
Contacto para comunicações de emergência	[Indique aqui]

Responder

Algo de estranho está a acontecer com o computador de um colaborador, que não sabe o que fazer. Esta situação equivale a sentir o cheiro de fumo ou a ver uma pequena chama na sala do café.

O que deve fazer:

1. **Isole o problema**: retire imediatamente o dispositivo da rede
2. **Identifique o tipo de incidente** e tome a seguinte medida:

   - ✓ Malware - retire o dispositivo imediatamente da rede
   - ✓ Roubo de credenciais – desative mas não elimine a conta e redefinia a palavra-passe
   - ✓ Violação de dados – ligue para o contacto de emergência de TI

- ✓ Ransomware: retire imediatamente o dispositivo da rede
- ✓ Ataque Denial of Service: contacte o gestor de TI e/ou a pessoa de contacto de suporte técnico externo

3. Determine o âmbito do incidente ao colocar estas perguntas:
   - ✓ Quando é que o incidente ocorreu?
   - ✓ Quem sofreu o impacto?
   - ✓ Qual é a natureza técnica do incidente? Como é que ocorreu? Temos conhecimentos internos para o resolver?
   - ✓ Quem está a par do incidente?
   - ✓ Ainda está a decorrer?

4. **Determine se pode ser controlado internamente** de forma adequada ou se precisa de contactar o suporte de TI externo para assegurar que a falha de segurança é resolvida de forma adequada.
5. **Continue a avaliar se o problema volta a ocorrer.** Caso seja pouco claro se o problema foi resolvido, peque por excesso e contacte um especialista para obter suporte.

Faça um resumo da forma como planeia isolar, identificar e determinar o âmbito de um incidente.

Recuperar

A crise passou e chegou o momento de as coisas voltarem ao normal. O âmbito do incidente e a gravidade do impacto determinarão quanto tempo e esforço serão necessários para a recuperação. No entanto, os passos básicos são os mesmos.

O que deve fazer.

1. Notifique todas as partes afetadas
2. Reponha o ID de utilizador e a palavra-passe do dispositivo comprometido
3. Aplique correções a todos os dispositivos
4. Volte a instalar o software e os dados a partir das cópias de segurança conforme necessário

Forneça abaixo um resumo da sua política e do plano de recuperação de um incidente para análise.

Recursos adicionais para a continuidade da atividade

À medida que continua a evoluir como organização, e a melhorar a sua cibersegurança e a resiliência, queremos fornecer-lhe duas ferramentas adicionais:

1. Árvore de decisão do plano de continuidade da atividade: ferramenta para orientá-lo nas principais decisões para fazer face a um incidente. Estão disponíveis espaços em branco para assegurar que está preparado.
2. Manual de procedimentos em caso de ransomware: Este guia tem como objetivo fornecer um roteiro para as empresas (por exemplo, pequenas e médias empresas, governos estaduais e locais) se protegerem contra esta ameaça crescente.

Formação e sensibilização dos colaboradores

Está na altura de reunir os conhecimentos que adquiriu ao longo do Programa e partilhá-los com os seus colegas. Como Líder cibernético da sua organização, irá introduzir mudanças duradouras na sua organização e na cadeia de valor global em geral.

Nesta secção, incluímos recursos chave para o ajudar a comunicar as melhores práticas de preparação para o ciberespaço em toda a sua organização de forma a promover uma mudança significativa. Encontrará modelos de e-mail que poderá copiar e personalizar, e listas de verificação para partilhar para todos os membros da sua organização poderem ser responsabilizados, bem como ligações a recursos adicionais, tanto do CRI como de toda a comunidade de cibersegurança, que podem fornecer orientações adicionais para a sua equipa.

A implementação é a etapa mais importante do Programa de prontidão cibernética porque é o momento em que o conhecimento se transforma em ação. Para o ajudar neste processo, fornecemos os seguintes recursos para utilizar:

1. Modelos de e-mail: utilize estes modelos para apresentar aos seus colaboradores os 4 principais problemas de cibersegurança e outros conceitos chave.

2. Módulos de formação sobre os 4 principais problemas de cibersegurança: vídeos de formação breves sobre os 4 principais problemas de cibersegurança que podem ser facilmente distribuídos aos colaboradores

3. PowerPoints de formação: PowerPoints para as sessões de formação dos colaboradores

4. Materiais partilháveis: cartazes, campanhas nas redes sociais, guias, etc.

O CRI concluiu que uma abordagem de grande interação é a melhor forma de maximizar os resultados da formação. Comunique claramente com os colaboradores não só o valor para a empresa, mas também para eles próprios, que a conclusão da ciberformação poderá oferecer os melhores resultados.

Tenha em conta a dimensão e o número de colaboradores da sua empresa quando decidir o melhor método de comunicação. Os debates presenciais, a comunicação por e-mail ou inclusivamente os Webinars agendados para acompanhar e auxiliar os colaboradores durante o processo de formação garantirão altas taxas de conclusão.

Documento de certificação de formação

O Cyber Readiness Institute exige que todos os colaboradores e contratantes recebam formação para obterem a Certificação de prontidão cibernética.

Ao assinar e devolver este Formulário de certificação, confirma que todos os colaboradores e contratantes receberam formação nas Políticas dos 4 principais problemas de cibersegurança do CRI e no seu papel no Plano de continuidade da atividade.

_____	_____
CEO	Líder cibernético
_____	_____
Data de assinatura	Data de assinatura

Recursos de formação

Modelos de e-mail: Os seguintes modelos de e-mail podem ser modificados e distribuídos a todos os colaboradores para os notificar sobre a sua nomeação para a função de Líder cibernético, as novas políticas cibernéticas da organização e os requisitos de formação futuros. É importante que o seu CEO envie o primeiro e-mail para os colaboradores compreenderem a importancia deste esforço.

1

Assunto: Mensagem da direção para os colaboradores sobre Prontidão cibernética

Olá, equipa,

Os ciberataques são ameaças muito reais e presentes para [Nome da empresa] e para as empresas que fornecemos. É de importância vital para o futuro da nossa atividade conseguirmos melhorar já a nossa prontidão cibernética. É por isso que estabelecemos uma parceria com o Cyber Readiness Institute para proteger os dados de [Nome da empresa], os dados dos nossos clientes e as suas informações pessoais para não serem expostos e usados para fins maliciosos.

Nomeei [Nome completo] como nosso(s) Líder(es) cibernético(s). A orientação da nossa equipa ao longo do Programa de prontidão cibernética será feita por [Ele/Ela/Eles], que adotará uma abordagem prática para aumentar a sensibilização para a cibersegurança ao focar-se no comportamento humano. Ao longo do Programa, vamos abordar as ciberameaças comuns à nossa empresa e desenvolver um Manual de prontidão cibernética para nos defendermos delas.

A realidade é que um simples clique numa ligação de e-mail suspeita pode permitir que um hacker aceda à nossa rede, acedendo assim aos dados da nossa empresa, aos dados dos nossos clientes e às suas informações pessoais. Estou empenhado em tornar a [Nome da empresa] mais resistente à cibersegurança ao prevenir os ataques e ao estar preparada quando ocorre um. Agradecemos que se tenha juntado no apoio a [Nome completo] para assegurar que [Nome da empresa] está preparada para o ciberespaço.

Muito obrigado,

[Assinatura do CEO]

2

Assunto: Novas políticas de sensibilização e formação em segurança

Olá, equipa!

[NOME ORGANIZAÇÃO] está a preparar-se para a Cibersegurança! O que significa para nós:

- Novas políticas para colaboradores: adicionámos algumas novas políticas e protocolos ao nosso manual que oferecem procedimentos e diretrizes para melhorar a segurança da [NOME DA ORGANIZAÇÃO]. Poderá analisar estas políticas aqui. [LIGAÇÃO]
- Líder cibernético designado: uma pessoa responsável por liderar o nosso percurso de prontidão cibernética.

Poderá estar a perguntar-se o que significa "Prontidão cibernética". "Prontidão cibernética" significa ser inteligente em relação aos hábitos tecnológicos e saber o que procurar para se manter seguro.

Os cibercriminosos sabem como a maioria de nós trabalha e exploram estes hábitos comuns para ultrapassar a sofisticada tecnologia de cibersegurança. De facto, alguns comportamentos estão na origem da maioria das falhas de cibersegurança e da forma como os hackers conseguiram entrar. Felizmente, quando sabemos o que fazer e o que não fazer em relação a estes 4 principais problemas de cibersegurança, a probabilidade destes métodos de ataque terem êxito diminui drasticamente.

- Palavras-passe+
- Atualizações de software
- Phishing
- Armazenamento e partilha de dados

Bloquear estas quatro áreas significa que os dados confidenciais relacionados com os clientes, fornecedores e colaboradores da [NOME DA ORGANIZAÇÃO] estão mais seguros. É por esta razão que vamos enviar alguns e-mails breves que darão alguma formação básica sobre as 4 principais problemas de cibersegurança e as coisas simples que todos podemos fazer para os evitar e prevenir.

Tenha em atenção que a adesão à política de cibersegurança e a formação são *obrigatórias*. Estes e-mails e pedidos devem demorar apenas 10 a 15 minutos a concluir, e solicitamos que responda ao seu superior hierárquico direto depois de concluir cada sessão de formação.

O primeiro e-mail de formação será enviado a [MM/DD]. Entretanto, leia as políticas atualizadas para saber mais sobre este esforço.

Em caso de dúvida sobre este assunto, contacte-nos!

[ASSINATURA DE E-MAIL]

3

Assunto: Problema cibernético principal n.º 1: Palavras-passe+

Olá, equipa!

É a nossa primeira sessão da série de formação Programa de prontidão cibernética!

Problema cibernético principal n.º 1: Palavras-passe+

A palavra-passe é uma porta de entrada para uma rede, um indivíduo ou uma organização. Utilizamos centenas de palavras-passe e dispositivos ligados na nossa vida profissional e pessoal, cada um deles uma porta de entrada para a nossa empresa. Uma palavra-passe fraca equivale a deixar a porta destrancada.

Cada uma das nossas palavras-passe é guardiã das informações e de sistemas importantes que nos são confiados, e pelos quais somos responsáveis. Não podemos deixar que sejam alvos fáceis.

Uma palavra-passe difícil de decifrar é a primeira linha de defesa contra hackers oportunistas. Criar uma palavra-passe forte demora apenas alguns segundos e é algo que todos os colaboradores da [NOME DA ORGANIZAÇÃO] terão de fazer para ajudar a manter os nossos dados tão seguros quanto possível.

Segue-se uma formação rápida sobre como criar palavras-passe fortes que poderá memorizar e utilizar facilmente:

[LIGAÇÃO]

Também atualizámos as políticas da nossa empresa em matéria de palavras-passe, que se aplicam a todos os colaboradores e contratantes da [ORGANIZAÇÃO].

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as suas palavras-passe, não hesite em contactar-me diretamente para falarmos sobre o assunto.

[ASSINATURA DE E-MAIL]

4

Assunto: Problema cibernético principal n.º 2: Atualizações de software

Olá, equipa!

Estamos na segunda sessão da nossa série de formação sobre o Programa de prontidão cibernética!

Problema cibernético principal n.º 2: Atualizações de software

É provável que esteja familiarizado com as notificações pop-up que informam que está disponível uma atualização de software para o seu computador, portátil, tablet ou dispositivo móvel. Apesar de poder ser tentador clicar em "Lembrar-me mais tarde", esta não é uma boa ideia. As atualizações de software reparam as falhas de segurança importantes e corrigem os erros críticos que foram identificados, pelo que devem ser instaladas imediatamente.

A não instalação destas atualizações deixa a porta aberta a vulnerabilidades de segurança conhecidas que os cibercriminosos podem e vão explorar para entrar e fazer um ataque. O infame ataque do ransomware WannaCry tirou partido de uma falha de segurança identificada no sistema operativo Windows que já tinha sido corrigida numa atualização dois meses antes. Apesar de o ataque só ter afetado quem não tinha instalado a atualização, em apenas 24 horas mais de 230.000 sistemas foram comprometidos e causaram danos globais de 4 mil milhões de dólares.

A instalação de atualizações pode eliminar estes pontos de acesso fácil e proteger contra ataques de malware e ransomware. Felizmente, as atualizações de software são fáceis de fazer.

A maioria dos sistemas operativos e do software pode ser configura para a "atualização automática", o que pode automatizar a instalação de atualizações e minimizar a interrupção do seu trabalho. Bastam alguns minutos para assegurar ou ativar a "atualização automática" de aplicações, sistemas e dispositivos, pelo que o deve fazer o mais rapidamente possível.

Tal como fizemos com as palavras-passe, também revimos as nossas políticas empresariais relacionadas com as atualizações de software. Estes padrões aplicam-se a todos os colaboradores e contratantes da [[ORG]].

O PDF em anexo da Lista de verificação de atualização de software fornece instruções passo a passo e ligações para facilitar a sua realização, que pode ler aqui [LIGAÇÃO].

Tenha em atenção que a adesão à política e o preenchimento da Lista de verificação de atualização de software em PDF é *obrigatória* para todos os colaboradores da [ORGANIZAÇÃO]. Esta lista de verificação deve demorar apenas 10 a 15 minutos e deve ser preenchida até [MM/DD]. Não se esqueça de informar o seu superior hierárquico depois de preencher esta lista de verificação.

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as atualizações de software, não hesite em contactar-me diretamente para falarmos sobre o assunto.

[ASSINATURA DE E-MAIL]

5

Assunto: Problema cibernético principal n.º 3: Phishing

Olá, equipa!

Está pronto para a terceira sessão da nossa série de formação no Programa de prontidão cibernética?

Problema cibernético principal n.º 3: Phishing

O phishing é um dos ciberataques mais generalizados. Qualquer pessoa com uma conta de e-mail ou um smartphone pode receber um e-mail ou uma mensagem de texto com phishing. Os ataques de phishing recorrem a mensagens enganosas para obter informações confidenciais ou o acesso a uma rede. Estas mensagens tentam enganar as pessoas para clicarem numa ligação, descarregarem um anexo na mensagem ou até fornecerem diretamente informações confidenciais, tais como dados bancários.

Muitos nós sabemos que o príncipe nigeriano que lhe envia um e-mail a pedir uma transferência bancária de 5000 dólares para a sua conta bancária é uma fraude. Mas os esquemas de phishing são muitas vezes sofisticados e difíceis de detetar, se não soubermos a que aspetos devemos estar atentos. Estas mensagens costumam ser oportunistas, assumindo fraudulentamente a forma de comunicações reais que podemos receber legitimamente.

De facto, 9 em cada 10 ciberataques começam com phishing, dada a eficácia com que os hackers o fazem. Embora os métodos que os hackers utilizam para lançar ataques de phishing estejam sempre a evoluir, a maioria das mensagens de phishing utiliza uma série de truques que pode aprender a detetar para não ser enganado.

Veja este breve vídeo para aprender alguns truques para detetar "phishing" nas suas mensagens. [LIGAÇÃO PARA O VÍDEO]

Além disso, veja mais alguns truques para detetar uma tentativa de phishing [AQUI].

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as atualizações de software, não hesite em contactar-me diretamente para falarmos sobre o assunto.

[ASSINATURA DE E-MAIL]

6

Assunto: Problema cibernético principal n.º 4: Armazenamento e partilha seguros

Olá, equipa!

Hoje vamos abordar a última questão central do ciberespaço na nossa série de formação no Programa de prontidão cibernética!

Problema cibernético principal n.º 4: Armazenamento e partilha seguros

As unidades USB são uma forma popular e fácil de armazenar e transportar ficheiros, mas também são alvos fáceis do software malicioso.

Os hackers podem infetar as unidades USB com software malicioso, tal como vírus, spyware e muitos outros, que podem causar danos irreversíveis. Alguém que encontre uma unidade USB "perdida" no parque de estacionamento pode ligá-la ao seu computador para ver o que contém e devolvê-la ao proprietário, sem conhecer o risco antes que seja tarde demais. As unidades USB não são o único tipo de dispositivo multimédia amovível, também se incluem:

- Discos óticos (discos Blu-Ray, DVDS e CD-ROMs)
- Cartões de memória (cartão Compact Flash, cartão Secure Digital e pen USB)
- Discos Zip/Disquetes
- Unidades flash USB
- Discos rígidos externos (DE, EIDE, SCSSI e SSD)
- Câmaras digitais
- Smartphones
- Outros dispositivos externos/acopláveis que contêm funcionalidades de suportes amovíveis

Atualizámos a nossa política da empresa relativa ao armazenamento e partilha de dados, que se aplicará a todos os colaboradores e contratantes da [ORGANIZAÇÃO]:

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as atualizações de software, não hesite em contactar-me diretamente para falarmos sobre o assunto.

Na próxima semana, iremos abordar o nosso novo Plano de resposta a incidentes, que nos ajudará a preparar e a responder aos eventos e problemas cibernéticos que poderão ocorrer.

[ASSINATURA DE E-MAIL]

7

Assunto: O nosso Plano de continuidade de atividade

Olá, equipa!

Vamos hoje abordar o nosso Plano de continuidade da atividade!

Isto servirá de roteiro para a nossa empresa como um todo e para cada pessoa determinar o que deve fazer e como agir quando ocorre um problema cibernético ou de segurança.

As práticas de higiene cibernética que aprendemos durante esta formação e as nossas novas políticas de prontidão cibernética contribuem muito para a redução do risco de uma falha da segurança. Mas mesmo com as melhores medidas implementadas, é importante assumir que provavelmente teremos de lidar com um incidente de segurança a dada altura.

O nosso Plano de continuidade da atividade permite-nos responder, resolver e aprender rapidamente com todos os problemas que surgem. Uma crise pode ser caótica e causar uma grande tensão, mas ter um plano passo a passo assegura que a nossa resposta a uma falha de segurança é estratégica e eficaz, em vez de reativa ou inútil.

Existem três elementos principais para a continuidade da atividade:

Preparar

- ✓ Certifique-se sempre de que tem cópias de segurança atualizadas e de que sincroniza as contas na cloud
- ✓ Esteja sempre alerta para situações suspeitas ou estranhas

Responder

- ✓ Contacte sempre o [LÍDER CIBERNÉTICO OU CONTACTO DE TI] se detetar algo estranho ou suspeito (o computador ficou bloqueado depois de abrir um ficheiro, etc.)
- ✓ Deixe imediatamente de utilizá-lo e desligue o dispositivo da rede

Recuperar

- ✓ Notifique todas as partes afetadas
- ✓ Reponha todas as palavras-passe e IDs
- ✓ Reinstale o software, as contas sincronizadas e as cópias de segurança dos dados, conforme necessário

Atualizámos o manual de procedimentos da nossa empresa com este Plano de continuidade da atividade. Este plano *deve ser consultado e usado* por todos os colaboradores e contratantes da [[ORGANIZAÇÃO]], e estará disponível aqui [LIGAÇÃO].

Se tiver alguma dúvida sobre o nosso Plano de continuidade da atividade, não hesite em contactar-me diretamente para o debater. Na próxima semana, faremos uma breve recapitulação do que aprendemos durante este programa e, em seguida, a [ORGANIZAÇÃO] receberá oficialmente a Certificação de prontidão cibernética!

[ASSINATURA DE E-MAIL]

8

Assunto: Recapitulação da prontidão cibernética

Olá, equipa!

Concluímos a série de formação no Programa de prontidão cibernética! Vamos analisar rapidamente o que aprendemos no nosso percurso para a Prontidão cibernética.

Vídeo sobre os 4 principais problemas de cibersegurança

Vídeo do Plano de continuidade da atividade

Como sempre, não hesite em contactar-me diretamente para debater qualquer questão.

[ASSINATURA DE E-MAIL]

Recursos adicionais para a formação e a sensibilização dos colaboradores

Vídeos de formação

Seguem-se 6 vídeos breves sobre os 4 principais problemas de cibersegurança e o seu Plano de Continuidade de Negócio no YouTube da CRI. Partilhe estes vídeos com os colaboradores para os manter informados e envolvidos no desenvolvimento da cultura cibernética da sua organização.

Introdução aos 4 principais problemas de cibersegurança

Palavras-passe+

Atualizações de software

Sensibilização para o phishing

Armazenamento e partilha seguros

Plano de continuidade da atividade

Modelo do PowerPoint

Este modelo fornece os elementos básicos necessários para ministrar uma sessão de formação presencial, virtual ou híbrida para os seus colaboradores. Bastam algumas modificações rápidas para ter uma apresentação para os colaboradores sobre as políticas e os procedimentos de prontidão cibernética da sua organização.

Modelo de formação do CRI

Recursos adicionais

Ao longo dos últimos anos, o CRI desenvolveu outros conteúdos que poderão ser úteis na sua função enquanto Líder cibernético. Utilize os recursos para dar formação aos seus colaboradores e ampliar os seus conhecimentos sobre diferentes tópicos relacionados com a cibersegurança.

Kit de iniciação à prontidão cibernética: Formação de colaboradores para a sensibilização para a cibersegurança(cyberreadinessinstitute.org)

Cartazes de formação

Kit de Iniciação do CRI

Recursos de prontidão cibernética: Ferramentas de cibersegurança para PME (cyberreadinessinstitute.org)

Perguntas frequentes sobre seguros cibernéticos: Cyber Readiness Institute

Um bom Líder cibernético compreende que a prontidão cibernética não é mais uma caixa a preencher, mas sim uma prática e um hábito contínuos em que os colaboradores podem ver o valor e o panorama geral, apreciar o impacto que têm na segurança enquanto indivíduos, compreender as aplicações de segurança pessoal e sentir-se capacitado para fazer perguntas e alterar comportamentos. É por isso que queremos fornecer-lhe alguns recursos externos adicionais de parceiros de confiança para poder continuar o seu percurso de preparação cibernética.

Cyber Guidance for Small Businesses | CISA

Cross-Sector Cybersecurity Performance Goals | CISA

CISA Insights: Guidance for MSPs and Small- and Mid-sized Businesses | CISA

Multifactor Authentication (MFA) Toolkit | CISA

CISA Regions | CISA

Secure by Design, Secure by Default | CISA

Infografia sobre phishing (cisa.gov)

Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency CISA

Avoiding Social Engineering and Phishing Attacks | CISA

Incident Response Training | CISA

Cloud Vulnerability Management | CISA

The Business Case for Security | CISA

Free Cybersecurity Services and Tools | CISA

Além disso, consulte o Mastercard Trust Center, o Kit de ferramentas de cibersegurança para pequenas empresas da Global Cyber Alliance e o Índice de soluções cibernéticas para organizações sem fins lucrativos para obter vários recursos adicionais à medida que avança no seu percurso de prontidão cibernética:

Mastercard Trust Center | Cybersecurity Solutions for Every Business

Global Cyber Alliance's Cybersecurity Toolkit for Small Business

https://nonprofitcyber.org/nonprofit-cyber-solutions-index/

Celebrar e manter o seu êxito

É importante ter em conta que a prontidão cibernética não é uma solução pontual, mas sim uma prática contínua que deve ser constantemente reforçada. Para estarem preparados para o ciberespaço, os seus colaboradores devem praticar as políticas, os comportamentos e os bons hábitos de prontidão cibernética que foram debatidos todos os dias no Programa.

Incorporar estas melhores práticas para se tornarem um hábito será um processo para os colaboradores. Mesmo com uma boa formação inicial dos seus colaboradores, será necessário tempo, tenacidade e uma atitude positiva para manter uma cultura de prontidão cibernética.

Sugestões para manter a prontidão cibernética:

- Institua estas práticas no seu processo de integração de novos colaboradores para, à medida que o número de colaboradores cresce, a prontidão cibernética da organização expandir-se.
- Faça um inquérito pelo menos duas vezes por ano para avaliar o grau de sensibilização e consistência na sua organização.
- Verifique, avalie e lembre periodicamente os seus colaboradores, através de novas sessões de formação ou de campanhas por e-mail, com uma periodicidade mínima de dois anos.
- Utilize e implemente os guias e recursos do CRI para ajudar sua organização a continuar a melhorar a sua postura de segurança.

Os seus colaboradores estão agora capacitados sobre os 4 principais problemas de cibersegurança, e totalmente equipados com práticas e políticas que reduzem o risco de ciberataques! Caso ainda não o tenha feito, dedique um momento para reconhecer e valorizar estes esforços, bem como o impacto positivo que este trabalho terá na sua organização.

Lembre-se de que existem duas formas de utilizar o Manual de procedimentos:

1) Auto-conclusão e Receção do certificado de conclusão: Conclua este programa online ao seu próprio ritmo e utilize o Manual de procedimentos como uma ferramenta para o ajudar a adotar políticas chave, e a desenvolver um plano de continuidade empresarial para receber um certificado de conclusão.
2) Conclusão verificada e Receção da certificação de Prontidão cibernética do CRI: Conclua este Programa de prontidão cibernética online ao utilizar o Manual de procedimentos para adotar políticas chave, desenvolver um plano de continuidade da atividade, formar a sua força de trabalho e apresentar uma carta de certificação assinada. Em seguida, peça a um Formador de cibersegurança do CRI para analisar e verificar o seu Manual de procedimentos concluído.

Se estiver interessado em obter a Certificação de prontidão cibernética do CRI, contacte info@cyberreadinessinstitute.org. NÃO envie por e-mail ou qualquer outro serviço de transferência de dados este Manual de procedimentos para o CRI. Contacte-nos para tratarmos dos passos seguintes para a certificação.