CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Manual de estrategias de preparación cibernética

Una guía práctica para ayudar a reducir el riesgo cibernético y defenderse de los problemas de ciberseguridad más comunes.

Este manual de estrategias forma parte del Programa de preparación cibernética del Cyber Readiness Institute y se basa en las prácticas recomendadas de los principales expertos en ciberseguridad.

Una nota para el líder en ciberseguridad:

Primero, nos gustaría darle las gracias por dedicar su tiempo para completar el Programa de preparación cibernética. Este importante ejercicio ayudará a su organización a mejorar su resiliencia a los problemas cibernéticos comunes, y usted, como líder cibernético, es fundamental para que eso suceda.

Ahora es el momento de que aplique lo que ha aprendido en las primeras fases del programa e implemente cambios significativos dentro de su organización, a través de políticas y planes internos. Aquí, en el Manual de estrategias de preparación cibernética, hemos incluido una guía de políticas clara y procesable para cada uno de los problemas básicos de ciberseguridad. El documento contiene campos en blanco que se pueden completar, por lo que puede introducir el nombre y la información de su organización para personalizar estas políticas en el documento, y una lista de comprobación que le ayudará a supervisar su progreso. O, si lo prefiere, puede incorporar el lenguaje en sus materiales internos y personalizar el contenido para satisfacer las necesidades únicas de su organización.

Hay dos formas de utilizar el programa para mejorar la preparación cibernética de su organización. El primer enfoque es realizar el programa en línea usted mismo y compartir lo que aprenda con su organización. Si decide dar el siguiente paso, el segundo enfoque requiere que un instructor de ciberseguridad de CRI revise su manual de estrategias para verificar que haya implementado los requisitos de CRI.

> **1) Autocompletar + Recibir certificado de finalización:** Complete este programa en línea y utilice el manual de estrategias para adoptar políticas clave y desarrollar un plan de continuidad del negocio.
> **2) Finalización verificada + Recibir la certificación de preparación cibernética de CRI:** Complete este programa en línea, utilice el manual de estrategias para adoptar políticas clave y desarrollar un plan de continuidad del negocio, forme a sus empleados y envíe una carta de certificación firmada, y permita que un instructor de ciberseguridad de CRI revise y verifique su manual de estrategias completado.

Además, el manual de estrategias incluye directrices para crear un plan de continuidad del negocio. Incluso con la mejor higiene cibernética pueden producirse ataques. Si se producen, es importante tener un plan de acción claro para mitigar el impacto. Les invitamos a copiar el Plan de respuesta a incidentes en sus políticas internas. Así tendrán un marco procesable si es necesario.

Gracias nuevamente por su participación en el Programa de preparación cibernética. Les deseamos a ustedes y a su organización un gran éxito.

Acerca del programa

El Programa de preparación cibernética es una forma sencilla y práctica para que las organizaciones ofrezcan formación sobre seguridad a los empleados y establezcan prácticas de preparación cibernética sostenibles y efectivas. Diseñado específicamente para pequeñas y medianas empresas, este programa se centra en el comportamiento humano y le ayudará a crear una plantilla capacitada, educada y comprometida con prácticas eficaces de ciberhigiene que repercuten directamente en la seguridad y la viabilidad de su empresa.

Obtenga más información en: cyberreadinessinstitute.org

Tabla de contenido

Visión general del Programa de preparación cibernética

Abordar la causa raíz de los problemas de ciberseguridad

A medida que nuestro mundo está más conectado, las empresas se enfrentan a desafíos cada vez más complejos para proteger su información y tecnología, lo que hace que estar preparados cibernéticamente sea más importante que nunca. Los ciberagentes maliciosos aprovechan los hábitos comunes y los comportamientos predecibles para eludir incluso las tecnologías de seguridad más avanzadas. Es por eso que el Cyber Readiness Institute ha desarrollado un programa de formación centrado específicamente en el comportamiento humano.

El Programa de preparación cibernética es una forma sencilla y práctica para que su organización aumente la concienciación y establezca prácticas de preparación cibernética sostenibles y eficaces. El programa se ha diseñado específicamente para pequeñas y medianas empresas, y se centra en el comportamiento humano para ayudarlo a crear una plantilla capacitada, educada y comprometida con prácticas eficaces de ciberhigiene que repercuten directamente en la seguridad y la viabilidad de su empresa.

Programa gratuito

El programa es gratuito y requiere conocimientos técnicos mínimos para completarlo. Desde plantillas de políticas hasta materiales de formación, le ofrecemos todo lo que necesita para desarrollar sus conocimientos sobre ciberseguridad e involucrar a sus empleados para crear una organización preparada cibernéticamente.

Papel del líder en ciber-seguridad

Como líder en ciberseguridad, su función es influir positivamente en el comportamiento humano, crear concienciación y lograr el compromiso de los empleados, e involucrar a la alta dirección para crear una cultura de preparación cibernética de arriba a abajo en su organización.

Para ser un líder en ciberseguridad eficaz, debe tener buenas aptitudes de gestión e interpersonales, debe sentirse cómodo con la tecnología, debe tener capacidad para desempeñar su puesto, debe sentir pasión por la importancia de la ciberseguridad y debe recibir el apoyo de la dirección.

Los líderes en ciberseguridad saben que la preparación cibernética no es una casilla que se debe marcar una sola vez, sino una práctica y un hábito continuos donde los empleados pueden ver el valor y el panorama general, apreciar el impacto en la seguridad que tienen como individuos, conocer las aplicaciones de seguridad personal y sentirse capacitados para hacer preguntas y cambiar comportamientos con regularidad.

Como líder en ciberseguridad designado, aprenderá los conceptos básicos de la preparación cibernética, desarrollará políticas y procedimientos cibernéticos para su empresa y luego formará a los empleados de su empresa para obtener una certificación de preparación cibernética.

Si simplemente está aquí para obtener un certificado de finalización, puede completar el programa y el manual de estrategias por su cuenta sin enviar un manual para su certificación.

Si desea obtener la certificación de preparación cibernética, utilice la siguiente lista de comprobación mientras trabaja en el manual de estrategias para asegurarse de haber completado todos los requisitos antes de enviarlo a info@cyberreadinessinstitute.org.

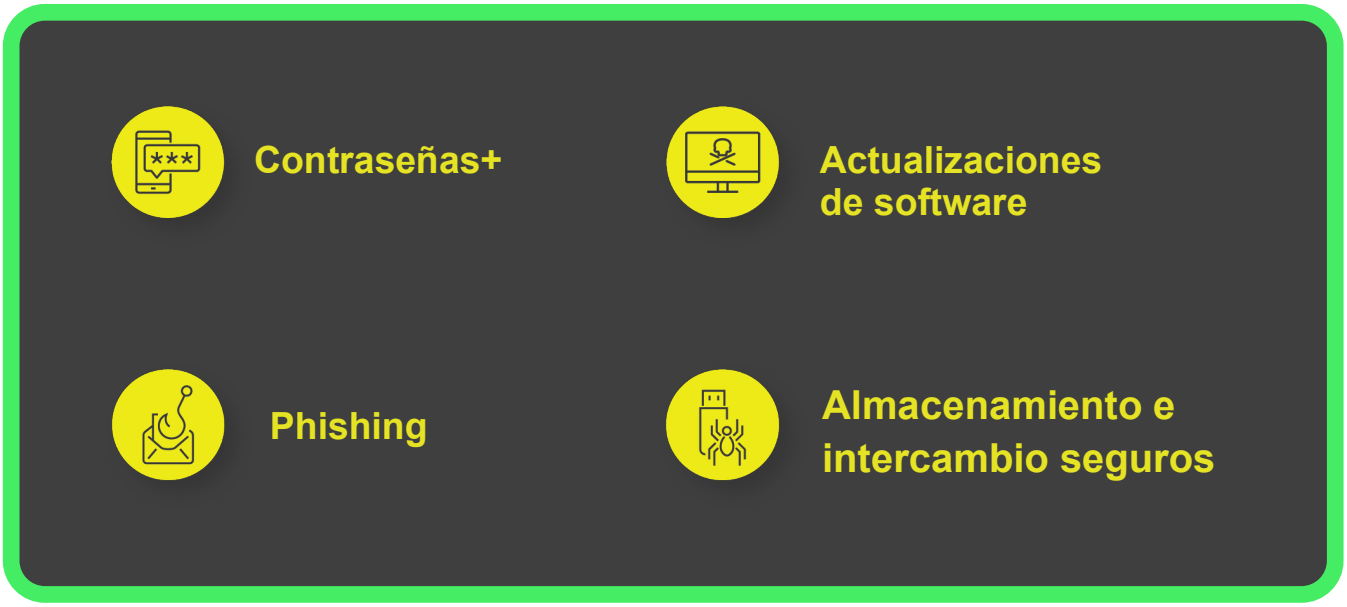
	Fecha de finalización	Notas
Líder en ciberseguridad designado e información de contacto documentada		
Métricas de referencia registradas		
Cuatro políticas básicas establecidas		
Herramienta de gestión de actualizaciones de software completa		
Hoja de trabajo de priorización completa		
Plan de respuesta a incidentes completo		
Formación de los empleados sobre las cuatro políticas básicas y continuidad del negocio completa		
Documento de certificación de formación firmado		
Métricas de reevaluación registradas		
Programa en línea de preparación cibernética completo		
Manual de estrategias enviado para revisión (si quiere obtener la certificación)		

Cuatro políticas básicas

El Programa de preparación cibernética se centra en cuatro políticas clave porque son la causa de la mayoría de los problemas de ciberseguridad y más fáciles de prevenir. La forma en que los empleados administran las contraseñas y la autenticación, las actualizaciones de software, la formación de concienciación sobre el phishing y los datos definen la posición de seguridad de una organización.

Estos requisitos de políticas son fáciles de implementar y gestionar para organizaciones de todos los tamaños. Proporcionar un nivel básico verificable de prácticas y procedimientos de ciberseguridad que todas las personas de su organización deben cumplir.

Estos requisitos deben aplicarse a todos los empleados y personal subcontratado que accedan a los sistemas y redes de la empresa en todos los dispositivos, incluidos ordenadores, teléfonos y tabletas. Esto se aplica a los dispositivos proporcionados por la empresa y a los dispositivos personales.



Acerca de las contraseñas

La autenticación y las contraseñas garantizan que las personas adecuadas tengan acceso a los sistemas, recursos e información adecuados que necesitan para hacer su trabajo todos los días. Algunos componentes clave incluyen contraseñas, preguntas de seguridad, autenticación multifactor y biometría (por ejemplo, escaneo de la huella dactilar o reconocimiento facial). Los empleados de su organización probablemente utilicen muchos sistemas y dispositivos diferentes que requieren una contraseña o alguna forma de autenticación. Esto incluye credenciales de cuenta, acceso a la base de datos, datos de inicio de sesión en el ordenador, nombres de usuario, insignias, etc.

Contraseñas+:

la primera línea de defensa contra los piratas informáticos oportunistas es la autenticación robusta, que consiste en contraseñas largas y el uso de la autenticación multifactor (MFA). Habilitar una autenticación robusta lleva solo unos minutos y es un elemento clave de una buena higiene cibernética. El compromiso de la organización de utilizar prácticas de autenticación robustas garantizará que solo las personas adecuadas tengan acceso a los sistemas, recursos e información adecuados.

Requisitos de la política de CRI:

1. La MFA debe estar habilitada en todo el hardware y software que lo admita.
2. Las contraseñas deben tener al menos 15 caracteres. Si una aplicación o dispositivo no permite 15 caracteres, las contraseñas deben tener la longitud máxima permitida.
3. No es necesario cambiar las contraseñas periódicamente. Si existen pruebas de una infracción de ciberseguridad, todas las contraseñas deben cambiarse de inmediato.

Acerca de las actualizaciones de software

Las correcciones de seguridad en las actualizaciones de software se denominan "parches". Estos parches tapan los agujeros de seguridad de las vulnerabilidades identificadas que los piratas informáticos pueden aprovechar. La gran mayoría de los ciberataques se dirigen a sistemas que tienen vulnerabilidades conocidas que se han solucionado en una actualización de software que simplemente no se había instalado y que podrían haberse evitado si las actualizaciones se hubieran implementado.

Actualizaciones de software:

La mayoría de los ciberataques se dirigen a sistemas con vulnerabilidades conocidas. La actualización periódica del software garantiza que las características de seguridad más recientes funcionen para usted.

Requisitos de la política de CRI:

1. Desarrollar un proceso de actualización de software utilizando la herramienta de gestión de actualizaciones de software de CRI

Acerca del phishing

El phishing es un ataque cibernético que utiliza correos electrónicos y mensajes engañosos para obtener acceso a la red de una organización. El phishing se dirige a las personas engañando al destinatario del correo electrónico o del texto para que haga clic en un enlace o descargue un archivo adjunto que puede infectar ese dispositivo con malware o que puede permitir que un pirata informático obtenga acceso a los sistemas o cuentas de una persona. Estos mensajes suelen ser oportunistas, disfrazados de comunicaciones reales que una persona puede recibir legítimamente.

Phishing:

El phishing utiliza mensajes engañosos para obtener acceso a la red y los datos de una organización. Cualquiera que tenga una cuenta de correo electrónico o un smartphone puede poner en peligro a su organización al hacer clic en enlaces incluidos en mensajes de phishing. Para disminuir el riesgo de que un intento de phishing tenga éxito, los empleados deben completar una formación de concienciación adecuada de manera regular para mantenerse actualizados sobre la naturaleza cambiante de esta amenaza.

Requisitos de la política de CRI:

1. Comunicaciones de concienciación sobre phishing enviadas a todos los empleados mensualmente.
2. Todos los empleados deben completar con éxito un curso trimestral sobre phishing que incluya como mínimo: concienciación, ejemplos y métodos de respuesta.
3. Los nuevos empleados deben completar con éxito el curso sobre phishing como parte de su proceso de incorporación o dentro de los 30 días posteriores a su fecha de inicio.

Acerca del almacenamiento e intercambios seguros

La forma en que almacena y comparte documentos y datos en la red informática de su organización es fundamental para estar preparado para la ciberseguridad. Las copias de seguridad periódicas y una política de USB sólida son esenciales para mantener su organización segura y resiliente.

Almacenamiento e intercambio seguros:

Los USB y otras formas de medios extraíbles son portadores comunes de virus y malware. Establecer políticas y directrices sólidas para los dispositivos USB y medios extraíbles ayudará a mantener los datos seguros y evitar ataques innecesarios. Con el almacenamiento en la nube, su organización puede almacenar datos en Internet a través de un proveedor que administra y opera el almacenamiento de datos como un servicio.

Requisitos de la política de CRI:

1. Prohíba el uso de USB y dispositivos de medios extraíbles excepto en casos críticos preestablecidos para el negocio. (Consulte Consejos, trucos y directrices para ver ejemplos).
2. Priorice el almacenamiento en la nube para la transferencia y el almacenamiento de archivos en todas las aplicaciones cuando estén disponibles.
3. Active el cifrado automático para la transferencia y el almacenamiento de archivos en todas las aplicaciones cuando esté disponible.
4. Se debe realizar una copia de seguridad periódica de todos los datos empresariales críticos utilizando medios extraíbles seguros y fiables o almacenamiento en la nube seguro y fiable.

Políticas de ciberseguridad de [su organización]

Instrucciones de uso:

Se debe utilizar la siguiente plantilla de políticas para desarrollar o registrar las políticas de ciberseguridad de su organización.

Si su organización aún no tiene políticas de ciberseguridad, simplemente puede añadir su logotipo a la plantilla de CRI y utilizar las nuestras.

Si su organización ya tiene políticas de ciberseguridad que cumplan o superen los requisitos de CRI, use la siguiente plantilla para registrarlas para su revisión.

Contraseñas:

Nombre de la política	Detalles de la política

Actualizaciones de software:

Nombre de la política	Detalles de la política

Phishing:

Nombre de la política	Detalles de la política

Intercambio seguro de archivos:

Nombre de la política	Detalles de la política

Herramienta de administración de actualizaciones de software

Instrucciones de uso:

Esta herramienta le ayudará a realizar un seguimiento de las actualizaciones de software necesarias para mantener su organización funcionando de forma segura. Utilice esta herramienta para enumerar el software que utiliza su organización y que requiere la aplicación de actualizaciones. Esta herramienta no está destinada a inventariar ni realizar un seguimiento de las actualizaciones de software en los distintos dispositivos, pero recuerde que debe formar a los empleados sobre la importancia de habilitar las actualizaciones automáticas. Piense en los diferentes tipos de software que utiliza, como, por ejemplo: sistemas (Windows, MacOS), aplicaciones (Office 365, QuickBooks) y otros (Zoom, antivirus).

1. Enumere el software que utiliza su organización en la columna A. Puede utilizar los ejemplos que se incluyen en la hoja de trabajo como punto de partida. Añada una fila para cualquier software que utilice y que no esté en la lista, y elimine las filas de los programas de software que no utiliza su empresa.

2. Determine quién es responsable de la actualización del software en la columna B. ¿Es el departamento de TI, el proveedor, etc.?

3. Indique quién utiliza el software (todos los empleados, marketing, ventas, contabilidad) en la columna C.

4. Ahora que tiene esta lista, haga una clasificación rápida para identificar si el software tiene una prioridad alta, media o baja para su negocio principal. Consulte la hoja de trabajo de priorización de su plan de continuidad del negocio para clasificar la prioridad de cada software en la columna D.

5. Utilice la información de las columnas B a D para determinar si las actualizaciones automáticas deben habilitarse en la columna E. En caso de duda, actívelas.

6. Si las actualizaciones automáticas no están habilitadas, puede utilizar esta herramienta periódicamente para registrar la fecha de la última actualización realizada en la columna F.

Software	¿Quién es responsable de actualizarlo?	¿Quién lo usa?	Prioridad	Actualizaciones automáticas habilitadas	Fecha de finalización de la última actualización
Apple iOS	Usuario	Todos los empleados	Alta	Sí	
MacOS					
Microsoft Windows					
Office 365					
PayPal					
QuickBooks					
Slack					
Square					
Xero					
Zelle					
Zoom					

Plan de continuidad del negocio

Un plan de continuidad del negocio ofrece a las empresas la oportunidad de planificar su capacidad de seguir proporcionando productos y servicios dentro de plazos aceptables con una capacidad predefinida durante una crisis. El plan respaldará los objetivos estratégicos, protegerá la reputación y la credibilidad, y permitirá mostrar resiliencia ante un ciberataque.

Desarrollar este plan le ayudará a adelantarse a la amenaza. Créanos cuando le decimos que no querrá tratar de averiguar cómo responder en medio de un incidente. El tiempo de respuesta es fundamental para minimizar el daño.

Para desarrollar su plan de continuidad del negocio deberá completar lo siguiente:

1. Hoja de trabajo de priorización: una herramienta que le permita inventariar los datos y la información que son más importantes para que su organización tenga éxito. Dar prioridad a lo que es más importante proteger le ayudará a crear políticas eficaces y a tomar decisiones de inversión inteligentes.

2. Plan de respuesta a incidentes: un plan integral paso a paso que le permita responder, resolver y aprender rápidamente de cada incidente.

Una herramienta de actualización de software y una política de copia de seguridad de los datos también son elementos clave que contribuyen a su resiliencia general.

También hay otros recursos adicionales en el manual de estrategias, incluidos más adelante, que lo ayudarán a fortalecer su ciberseguridad y resiliencia a medida que continúa mejorando la planificación de la continuidad del negocio de su organización.

Hoja de trabajo de priorización

Es hora de pensar en qué datos, software y hardware son más importantes para que su organización tenga éxito. Dar prioridad a lo que es más importante proteger le ayudará a crear políticas eficaces y a tomar decisiones de inversión inteligentes.

Enumere los datos que son más importantes para el éxito de su organización (números de tarjetas de crédito de los clientes, información personal de los empleados, datos financieros, etc.).

Enumere el software que es más importante para el éxito de su organización (Office365, MacOS, QuickBooks, etc.).

Enumere las herramientas de hardware y software que son más importantes para el funcionamiento de su organización (dispositivos móviles, ordenadores portátiles, impresoras, escáneres, etc.).

Identifique los tres o cinco elementos de las tres listas anteriores que causarían el mayor daño a su organización si se perdieran, fueran robados o no estuvieran disponibles.

Plan de respuesta a incidentes (IRP)

Establecer prácticas y políticas de preparación cibernética ayuda a reducir el riesgo, pero es importante asumir que es probable que nuestra empresa tenga que lidiar con un incidente de seguridad en algún momento que podría afectar a las operaciones comerciales. Tratar de determinar cómo responder en medio de un incidente no es una buena idea. El tiempo de respuesta es fundamental para minimizar el daño. Tener un plan claro puede marcar la diferencia entre un incidente y una catástrofe.

Un IRP integral paso a paso le permite responder, resolver y aprender rápidamente de cada incidente. Este IRP sirve como una hoja de ruta sobre qué hacer al responder a un incidente de ciberseguridad y garantizar de ese modo que tengamos una respuesta estratégica en lugar de reactiva.

Hay tres elementos principales en nuestra respuesta a incidentes:

1. **Prepararse** para un posible incidente futuro
2. **Responder** durante el incidente
3. **Recuperarse** del incidente

Prepararse

Pautas organizativas:

La inversión que realice en preparación le reportará grandes dividendos. Hay algunas acciones esenciales que deben realizarse lo antes posible para prepararse adecuadamente y reducir el daño de un ataque. CRI revisará y confirmará que haya incluido lo siguiente en su cuaderno de estrategia final.

1. **Designar un líder en ciberseguridad.** Designar un líder en ciberseguridad es esencial para la preparación cibernética de su empresa. Como líder en ciberseguridad, usted es responsable de compartir información de preparación cibernética con sus empleados y gestionar el desarrollo de sus políticas de preparación cibernética.

Medidas implementadas	Fecha de finalización

2. **Implementar cuatro políticas básicas:** asegúrese de que se establezcan y compartan políticas de ciberseguridad con los empleados que cumplan o superen los requisitos de CRI.

Medidas implementadas	Fecha de finalización

3. **Realice una copia de seguridad de los datos y asegúrese de que puede volver a instalar desde las copias de seguridad**. La recuperación de un ataque será mucho más rápida y afectará mucho menos a las operaciones si tiene copias de seguridad actuales del software de su sistema, las aplicaciones y especialmente de sus datos importantes. También querrá asegurarse de que cada persona de su organización tenga copias de seguridad si no lo hace de forma centralizada. Es importante probar periódicamente sus copias de seguridad.

Medidas implementadas	Fecha de finalización

4. **Formar a sus empleados.** Cada miembro del equipo debe saber cómo detectar actividades sospechosas y a quién contactar al respecto. Los empleados críticos también deben conocer cuál es su función en la respuesta a un incidente.

Medidas implementadas	Fecha de finalización

5. Establecer contactos. Establezca contactos internos y externos a los que pueda llamar si un incidente de ciberseguridad supera su capacidad de controlarlo.

Contacto de emergencia de TI	[Indíquelo aquí]
Proveedor de servicios de Internet	[Indíquelo aquí]
Contacto de emergencia legal	[Indíquelo aquí]
Contacto de emergencia de comunicaciones	[Indíquelo aquí]

Responder

Algo loco está sucediendo en el ordenador de un empleado y este no sabe qué hacer. La situación es equivalente a oler humo o ver una pequeña llama en la sala de café.

Esto es lo que debe hacer:

1. **Aislar el problema**: desconecte inmediatamente el dispositivo de la red
2. **Identificar el tipo de incidente** y realizar la siguiente acción:

   - ✓ Malware: desconecte el dispositivo de la red inmediatamente
   - ✓ Robo de credenciales: deshabilite la cuenta, pero no la elimine, y restablezca la contraseña
   - ✓ Violación de datos: llame al contacto de emergencia de TI
   - ✓ Ransomware: desconecte el dispositivo de la red inmediatamente

- ✓ Denegación de servicio: póngase en contacto con el responsable de TI o con la persona de contacto del servicio de soporte técnico externo

3. Determinar el alcance del incidente haciendo estas preguntas:
   - ✓ ¿Cuándo ocurrió el incidente?
   - ✓ ¿A quién ha afectado?
   - ✓ ¿Cuál es la naturaleza técnica del incidente? ¿Cómo ocurrió? ¿Tenemos conocimientos internos para abordarlo?
   - ✓ ¿Quién conoce el incidente?
   - ✓ ¿Sigue en curso?

4. **Determinar si se puede controlar adecuadamente internamente** o si necesita llamar a soporte de TI externo para asegurarse de que el ataque se gestione de manera adecuada.
5. **Seguir comprobando si el problema vuelve a ocurrir.** Si no está claro si el problema se ha resuelto, actúe con precaución y póngase en contacto con un experto sobre el problema.

Proporcione un resumen de cómo piensa aislar, identificar y determinar el alcance de un incidente.

Recuperarse

La crisis terminó y ahora es el momento de que las cosas vuelvan a la normalidad. El alcance del incidente y la gravedad del impacto determinarán cuánto tiempo y esfuerzo se necesitará para recuperarse. Sin embargo, los pasos básicos son los mismos.

Esto es lo que debe hacer:

1. Notificar a todas las partes afectadas

2. Volver a definir la identificación de usuario y la contraseña del dispositivo atacado
3. Aplicar parches a todos los dispositivos
4. Reinstalar el software y los datos de las copias de seguridad según sea necesario

Proporcione a continuación un resumen de su política y plan para recuperarse de un incidente para su revisión.

Recursos adicionales para la continuidad del negocio

A medida que continúa evolucionando como organización y mejora su ciberseguridad y resiliencia, queremos proporcionarle dos herramientas adicionales:

1. **Árbol de decisión del plan de continuidad del negocio:** una herramienta para guiarlo en las decisiones clave ante un incidente. Hay algunos espacios en blanco que debe completar para asegurarse de estar preparado.
2. **Manual de estrategias para actuar ante ataques de ransomware:** esta guía tiene como objetivo proporcionar una hoja de ruta para que las organizaciones (por ejemplo, pequeñas y medianas empresas, administraciones estatales y locales) se protejan de esta creciente amenaza.

Formación y concienciación de los empleados

Ahora es el momento de recopilar los conocimientos que ha adquirido a lo largo del programa y compartirlos con sus compañeros. Como líder en ciberseguridad de su organización, conseguirá realizar cambios duraderos en su organización y en la cadena de valor global en general.

En esta sección, hemos incluido recursos clave para ayudarlo a comunicar las prácticas recomendadas de preparación cibernética en su organización para impulsar un cambio significativo. Encontrará plantillas de correo electrónico que puede copiar y personalizar, listas de verificación que puede compartir para que todos los miembros de su organización rindan cuentas y enlaces a recursos adicionales, tanto de CRI como de toda la comunidad de ciberseguridad, que pueden ofrecer orientación adicional a su equipo.

La implementación es el paso más importante del Programa de preparación cibernética porque es el momento en que el conocimiento se convierte en acción. Para ayudarle en este proceso, le hemos proporcionado los siguientes recursos que puede usar:

1. Plantillas de correo electrónico: utilice estas plantillas para presentar a sus empleados las cuatro políticas básicas y otros conceptos clave.

2. Módulos de formación de las cuatro políticas básicas: vídeos cortos de formación de las cuatro políticas básicas que se pueden distribuir fácilmente a los empleados

3. Presentaciones en PowerPoint de formación: presentaciones en PowerPoint para sesiones de formación de empleados

4. Materiales compartibles: carteles, campañas en redes sociales, guías, etc.

CRI ha descubierto que un enfoque sumamente personalizado es la mejor manera de lograr los máximos resultados de la formación. Comunicar claramente a los empleados no solo el valor para la empresa, sino también para ellos mismos, que pueden aportar los cursos sobre ciberseguridad proporcionará los mejores resultados.

Cuando tenga que decidir cuál es el método de comunicación mejor, tenga en cuenta el tamaño de su empresa y la cantidad de empleados. Las conversaciones cara a cara, las comunicaciones por correo electrónico o incluso los seminarios web programados para realizar un seguimiento y ayudar a los empleados durante el proceso de formación garantizarán un alto porcentaje de finalización.

Documento de certificación de formación

El Cyber Readiness Institute exige que todos los empleados y personal subcontratado reciban formación para obtener la certificación de preparación cibernética.

Al firmar y devolver este formulario de certificación, usted confirma que todos los empleados y personal subcontratado han recibido formación sobre las cuatro políticas principales de CRI y su papel en el plan de continuidad del negocio.

_____	_____
CEO	Líder en ciberseguridad
_____	_____
Fecha de la firma	Fecha de la firma

Recursos de formación

Plantillas de correo electrónico: Las siguientes plantillas de correo electrónico se pueden modificar y distribuir a todos los empleados para notificarles su nombramiento para el puesto de líder en ciberseguridad, las nuevas políticas de ciberseguridad de la organización y los próximos requisitos de formación. Es importante que el CEO envíe el primer correo electrónico para que los empleados entiendan la importancia de esta iniciativa.

1

Asunto: Mensaje de la dirección a los empleados sobre la preparación cibernética

Hola, equipo:

Los ciberataques son amenazas muy reales y presentes para [Nombre de la empresa] y las empresas a las que ofrecemos servicio. Es de vital importancia para el futuro de nuestro negocio que mejoremos nuestra preparación cibernética ahora. Es por eso que nos hemos asociado con Cyber Readiness Institute para proteger los datos de [Nombre de la empresa], los datos de nuestros clientes y vuestra información personal para que no se vean expuestos ni se utilicen con fines maliciosos.

He designado a [Nombre completo] como nuestros líderes en ciberseguridad. [Él/ella/ellos/ellas] guiarán a nuestro equipo a través del Programa de preparación cibernética, que adopta un enfoque práctico para aumentar la concienciación sobre la ciberseguridad centrándose en el comportamiento humano. A lo largo del programa, explicaremos las ciberamenazas comunes que puede sufrir nuestra empresa y desarrollaremos un manual de preparación cibernética para defendernos de ellas.

La realidad es que simplemente hacer clic en un enlace de correo electrónico sospechoso puede permitir que un agente malicioso acceda a nuestra red, accediendo así a los datos de nuestra empresa, los datos de nuestros clientes y vuestra información personal. Me comprometo a hacer que [Nombre de la empresa] sea más resiliente a la ciberseguridad previniendo los ataques y estando preparados cuando ocurra alguno. Gracias por acompañarme para apoyar a [Nombre completo] para garantizar que [Nombre de la empresa] esté preparada para la ciberseguridad.

Muchas gracias,

[Firma del CEO]

2

Asunto: Nuevas políticas de concienciación y formación sobre seguridad

¡Hola, equipo!

¡[NOMBRE DE LA ORGANIZACIÓN] se está preparando para la ciberseguridad. ¿Qué significa esto para nosotros?:

- Nuevas políticas para empleados: hemos añadido algunas políticas y protocolos nuevos a nuestro manual que ofrecen procedimientos y pautas para mejorar la seguridad aquí en [NOMBRE DE LA ORGANIZACIÓN]. Podéis consultar estas políticas aquí. [ENLACE]
- Líder en ciberseguridad designado: una persona responsable de liderar nuestro viaje de preparación cibernética.

Quizás os preguntéis qué significa estar preparado para la ciberseguridad. Estar preparado para la ciberseguridad significa ser inteligente con respecto a los hábitos tecnológicos y saber qué buscar para mantenerse seguro.

Los ciberdelincuentes saben cómo trabajamos la mayoría de nosotros y aprovechan estos hábitos comunes para burlar la sofisticada tecnología de ciberseguridad. De hecho, algunos comportamientos son el origen de la mayoría de las vulneraciones cibernéticas y de cómo los delincuentes logran abrirse paso. Afortunadamente, cuando sabemos qué hacer y qué no hacer en relación con estos cuatro problemas principales de ciberseguridad, la posibilidad de que estos métodos de ataque tengan éxito disminuye drásticamente.

- Contraseñas+
- Actualizaciones de software
- Phishing
- Almacenamiento e intercambio de datos

Bloquear estas cuatro áreas significa que los datos confidenciales relacionados con los clientes, proveedores y compañeros de trabajo de [NOMBRE DE LA ORGANIZACIÓN] están más seguros. Es por eso que enviaremos algunos correos electrónicos breves que ofrecerán información básica sobre los cuatro problemas de ciberseguridad y las cosas simples que todos podemos hacer para evitarlos y prevenirlos.

Tened en cuenta que el cumplimiento de la política y la formación de ciberseguridad son *obligatorios*. Estos correos electrónicos y solicitudes solo deberían tardar entre 10 y 15 minutos en completarse, y os pedimos que contactéis con vuestro supervisor directo después de completar cada sesión de formación.

El primer correo electrónico de formación se enviará el [MM/DD]. Mientras tanto, podéis consultar las políticas actualizadas para obtener más información sobre esta iniciativa.

Si tenéis alguna pregunta sobre esto, poneos en contacto conmigo.

[FIRMA DE CORREO ELECTRÓNICO]

3

Asunto: Problema de ciberseguridad principal n.º 1: Contraseñas+

¡Hola, equipo!

Esta es la primera sesión de nuestra serie de cursos del Programa de preparación cibernética.

Problema de ciberseguridad principal n.º 1: contraseñas+

Una contraseña es una puerta a una red, a un individuo o a una organización. Usamos cientos de contraseñas y dispositivos conectados en nuestra vida profesional y personal, y cada uno de ellos es una puerta de acceso a nuestra empresa. Una contraseña débil es como dejar la puerta abierta.

Cada una de nuestras contraseñas es un guardián de la información y de los sistemas importantes en los que confiamos y de los que somos responsables. No podemos permitir que sean blancos fáciles.

La primera línea de defensa contra los piratas informáticos oportunistas es una contraseña difícil de descifrar. Crear una contraseña segura solo requiere unos segundos y es algo que todo empleado de [NOMBRE DE LA ORGANIZACIÓN] debe hacer para ayudar a mantener nuestros datos lo más seguros posible.

A continuación se ofrece un breve curso sobre cómo crear contraseñas seguras que puedas recordar y usar fácilmente:

[ENLACE]

También hemos actualizado las políticas de nuestra empresa sobre contraseñas, que se aplican a todos los empleados y personal subcontratado de [ORGANIZACIÓN].

Si tienes alguna pregunta sobre este curso o cómo usar y administrar tus contraseñas, no dudes en comunicarte conmigo directamente.

[FIRMA DE CORREO ELECTRÓNICO]

4

Asunto: Problema de ciberseguridad principal n.º 2: Actualizaciones de software

¡Hola, equipo!

Esta es la segunda sesión de nuestra serie de cursos del Programa de preparación cibernética.

Problema de ciberseguridad principal n.º 2: actualizaciones de software

Probablemente estés familiarizado con esas notificaciones emergentes que te indican que hay una actualización de software disponible para tu ordenador, portátil, tableta o dispositivo móvil. Aunque puede resultar tentador hacer clic en "Recordármelo más tarde", esta no es una buena idea. Las actualizaciones de software reparan importantes brechas de seguridad y corrigen errores críticos que se han identificado, y deben instalarse de inmediato.

No instalar estas actualizaciones deja la puerta abierta a vulnerabilidades de seguridad conocidas que los ciberdelincuentes pueden utilizar y utilizan para entrar y perpetrar un ataque. El infame ataque de ransomware WannaCry se aprovechó de un fallo de seguridad identificado en el sistema operativo Windows que ya se había solucionado en una actualización dos meses antes. Aunque el ataque solo afectó a aquellos que no habían instalado la actualización, en solo 24 horas más de 230.0000 sistemas se vieron comprometidos y causaron daños globales por valor de 4000 millones de dólares.

La instalación de actualizaciones puede eliminar estos puntos de fácil acceso y proteger de los ataques de malware y ransomware. Afortunadamente, las actualizaciones de software son fáciles de realizar.

La mayoría de los sistemas operativos y software se pueden configurar para que se actualicen automáticamente, lo que puede automatizar la instalación de actualizaciones y minimizar la interrupción de tu trabajo. Activar la actualización automática de aplicaciones, sistemas y dispositivos solo requiere unos minutos, así que hazlo lo antes posible.

Al igual que hicimos con las contraseñas, también hemos revisado las políticas de nuestra empresa en torno a las actualizaciones de software. Estos estándares se aplican a todos los empleados y personal subcontratado de [[ORGANIZACIÓN]].

El PDF con la lista de comprobación de actualización de software adjunto ofrece instrucciones paso a paso y enlaces para simplificar esta tarea y lo puedes leer aquí [ENLACE].

Ten en cuenta que cumplir la política y completar el PDF de lista de comprobación de actualización de software es *obligatorio* para todos los empleados de [ORGANIZACIÓN]. Solo tardarás entre 10 y 15 minutos en completar esta lista de comprobación y debes hacerlo antes del [MM/DD]. Asegúrate de informar a tu supervisor una vez que hayas completado esta lista de comprobación.

Si tienes alguna pregunta sobre este curso o sobre cómo usar y administrar las actualizaciones de software, no dudes en comunicarte conmigo directamente.

[FIRMA DE CORREO ELECTRÓNICO]

5

Asunto: Problema de ciberseguridad principal n.º 3: Phishing

¡Hola, equipo!

¿Listo para la tercera sesión de nuestra serie de cursos del Programa de preparación cibernética?

Problema de ciberseguridad principal n.º 3: phishing

El phishing es uno de los ciberataques más utilizados. Cualquiera que tenga una cuenta de correo electrónico o un smartphone puede recibir un mensaje de texto o correo electrónico de phishing. Los ataques de phishing utilizan mensajes engañosos para obtener información confidencial o acceder a una red. Estos mensajes intentan engañar a las personas para que hagan clic en un enlace, descarguen un archivo adjunto en el mensaje o incluso proporcionen directamente información confidencial, como datos bancarios.

La mayoría de nosotros sabemos que el príncipe nigeriano que envía un correo electrónico solicitando una transferencia bancaria de 5000 dólares a su cuenta bancaria es una estafa. Pero las estafas de phishing a menudo son sofisticada y difíciles de detectar si no sabemos qué buscar. Estos mensajes aparentan ser comunicaciones reales que una persona puede recibir legítimamente.

De hecho, 9 de cada 10 ciberataques comienzan con phishing porque los atacantes son expertos en estos ataques. Aunque los métodos que utilizan los estafadores para lanzar ataques de phishing siempre están evolucionando, la mayoría de los mensajes de phishing utilizan varios trucos que puedes aprender a detectar para no dejar que te engañen.

Mira este breve videoclip para aprender algunos trucos para detectar el "phishing" en tus mensajes. [ENLACE DE VÍDEO]

Además, consulta otros trucos para detectar un intento de phishing [AQUÍ].

Si tienes alguna pregunta sobre este curso o sobre cómo usar y administrar las actualizaciones de software, no dudes en comunicarte conmigo directamente.

[FIRMA DE CORREO ELECTRÓNICO]

6

Asunto: Problema de ciberseguridad principal n.º 4: almacenamiento e intercambio seguros

¡Hola, equipo!

Hoy explicamos el último tema principal de ciberseguridad en nuestra serie de cursos del Programa de preparación cibernética.

Problema de ciberseguridad principal n.º 4: almacenamiento e intercambio seguros

Los USB son una forma fácil y popular de almacenar y transportar archivos, pero también son blancos fáciles para el software malintencionado.

Los piratas informáticos pueden infectar los USB con software malicioso, como virus, spyware, etc., que puede causar daños irrevocables. Alguien que encuentre un USB "perdido" en el parking podría conectarlo a su ordenador para ver qué contiene y devolvérselo al propietario, sin conocer el riesgo antes de que sea demasiado tarde. Los USB no son el único tipo de dispositivo de medios extraíbles; también pueden incluir:

- Discos ópticos (discos Blu-Ray, DVD, CD-ROM)
- Tarjetas de memoria (tarjeta Compact Flash, tarjeta Secure Digital, stick de memoria)
- Discos Zip/Disquetes
- Unidades flash USB
- Discos duros externos (DE, EIDE, SCSSI y SSD)
- Cámaras digitales
- Smartphones
- Otros dispositivos externos/acoplables que contienen funciones de unidades multimedia extraíbles

Hemos actualizado nuestra política empresarial sobre almacenamiento e intercambio de datos, que se aplicará a todos los empleados y personal subcontratado de [ORGANIZACIÓN]:

Si tienes alguna pregunta sobre este curso o sobre cómo usar y administrar las actualizaciones de software, no dudes en comunicarte conmigo directamente.

La próxima semana hablaremos de nuestro nuevo plan de respuesta a incidentes, que nos ayudará a prepararnos y responder a eventos y problemas de ciberseguridad que puedan ocurrir.

[FIRMA DE CORREO ELECTRÓNICO]

7

Asunto: Nuestro plan de continuidad del negocio

¡Hola, equipo!

Hoy vamos a hablar de nuestro plan de continuidad del negocio.

Este plan servirá como un hoja de ruta para nuestra empresa en su conjunto y para que cada persona determine qué hacer y cómo actuar cuando ocurra un problema cibernético o de seguridad.

Las prácticas de higiene cibernética que hemos aprendido durante esta formación y nuestras nuevas políticas de preparación cibernética contribuyen en gran medida a reducir el riesgo de sufrir una vulneración de seguridad. Pero incluso con las mejores medidas implementadas, es importante asumir que probablemente tendremos que lidiar con un incidente de seguridad en algún momento.

Nuestro plan de continuidad del negocio nos prepara para responder, resolver y aprender rápidamente de cada problema que surja. Una crisis puede ser caótica y estresante, pero tener un plan paso a paso garantiza que nuestra respuesta a un ataque sea estratégica y efectiva en lugar de reactiva o inútil.

Hay tres elementos principales para la continuidad de nuestro negocio:

Prepararse

- ✓ Asegúrate siempre de mantener las copias de seguridad actualizadas y sincronizar las cuentas en la nube
- ✓ Mantente siempre alerta ante posibles actividades extrañas o sospechosas

Responder

- ✓ Contacta siempre con [LÍDER EN CIBERSEGURIDAD O CONTACTO DE TI] si detectas algo extraño o sospechoso (por ejemplo, el ordenador se bloquea después de abrir un archivo).
- ✓ Deja de usarlo inmediatamente y desconecta el dispositivo de la red

Recuperarse

- ✓ Notifica el problema a todas las partes afectadas
- ✓ Restablece todas las contraseñas e identificadores
- ✓ Reinstala el software, las cuentas sincronizadas y las copias de seguridad de datos según sea necesario

Hemos actualizado nuestro manual de empresa con este plan de continuidad del negocio. Todos los empleados *y personal subcontratado* de [[ORGANIZACIÓN]] deben consultar y usar este plan, al que puedes acceder aquí [ENLACE].

Si tienes alguna pregunta sobre nuestro plan de continuidad del negocio, no dudes en comunicarte conmigo directamente. La próxima semana, haremos un resumen rápido de lo que hemos aprendido durante este programa y luego [ORGANIZACIÓN] recibirá oficialmente la certificación de preparación cibernética.

[FIRMA DE CORREO ELECTRÓNICO]

8

Asunto: Resumen de preparación cibernética

¡Hola, equipo!

¡Ya hemos completado la serie de cursos del Programa de preparación cibernética! Dediquemos unos minutos a repasar rápidamente lo que hemos aprendido en nuestro viaje hacia la preparación cibernética.

El vídeo sobre los cuatro problemas de ciberseguridad principales

Vídeo del plan de continuidad del negocio

Como siempre, no dudes en ponerte en contacto conmigo directamente si tienes alguna pregunta.

[FIRMA DE CORREO ELECTRÓNICO]

Recursos adicionales para la formación y concienciación de los empleados

Vídeos de formación

Aquí hay seis vídeos cortos sobre las cuatro políticas principales y su plan de continuidad de negocio en el canal de YouTube de CRI. Comparta estos videos con los empleados para mantenerlos informados y comprometidos con el desarrollo de la cultura cibernética de su organización.

Introducción a las cuatro políticas básicas

Contraseñas+

Actualizaciones de software

Concienciación sobre el phishing

Almacenamiento e intercambio seguros

Plan de continuidad del negocio

Plantilla de PowerPoint

Esta plantilla proporciona los conceptos básicos de lo que necesitará para llevar a cabo una sesión de formación presencial, virtual o híbrida para sus empleados. Con solo unas cuantas modificaciones rápidas, tendrá una presentación para los empleados sobre las políticas y procedimientos de preparación cibernética de su organización.

Plantilla de formación de CRI

Recursos adicionales

En los últimos años, CRI ha desarrollado otros contenidos que pueden resultarle útiles en su función como líder en ciberseguridad. Utilice los recursos para formar a sus empleados y ampliar sus conocimientos sobre diferentes temas relacionados con la ciberseguridad.

Kit de inicio de preparación cibernética: formación para la concienciación de ciberseguridad de los empleados (cyberreadinessinstitute.org)

Carteles de formación

CRI Kit de inicio

Recursos de preparación cibernética: herramientas de ciberseguridad para pymes (cyberreadinessinstitute.org)

Preguntas frecuentes sobre seguros cibernéticos - Cyber Readiness Institute

Un buen líder en ciberseguridad sabe que la preparación cibernética no es una casilla que se debe marcar una sola vez, sino una práctica y un hábito continuos donde los empleados pueden ver el valor y el panorama general, apreciar el impacto en la seguridad que tienen como individuos, conocer las aplicaciones de seguridad personal y sentirse capacitados para hacer preguntas y cambiar comportamientos con regularidad. Es por eso que queremos ofrecerle algunos recursos externos adicionales de socios fiables que puede utilizar durante su viaje de preparación 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

Infografía 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

Además, consulte el Centro de confianza de Mastercard, el conjunto de herramientas de ciberseguridad para pequeñas empresas de la Global Cyber Alliance y el índice de soluciones cibernéticas para organizaciones sin fines de lucro para obtener un conjunto de recursos adicionales a medida que continúa su viaje de preparación 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 y mantener su éxito

Es importante señalar que la preparación cibernética no es una acción única, sino una práctica continua que debe reforzarse constantemente. Para estar preparado cibernéticamente, sus empleados deben practicar las políticas, comportamientos y buenos hábitos de preparación cibernética que se han explicado en el programa todos los días.

Incorporar estas prácticas recomendadas para que se conviertan en un hábito será un proceso para los empleados. Incluso con una buena formación de sus empleados, se necesitará tiempo, tenacidad y una actitud positiva para mantener una cultura de preparación cibernética.

Consejos para mantener la preparación cibernética:

- Haga que estas prácticas formen parte de su proceso de incorporación de nuevos empleados para que, a medida que su plantilla crezca, su preparación cibernética se expanda.
- Realice una encuesta al menos dos veces al año para medir la concienciación y la aplicación sistemática de estas prácticas en toda su organización.
- Registre, evalúe y recuerde periódicamente a su personal, ya sea a través de nuevas sesiones de formación periódicas o con campañas por correo electrónico al menos dos veces al año.
- Utilice e implemente guías y recursos de CRI para ayudar a su organización a continuar mejorando su posición de seguridad.

Su plantilla ahora está capacitada sobre los cuatro problemas de ciberseguridad principales y completamente equipada con prácticas y políticas que reducen el riesgo de que se produzcan ciberataques. Si aún no lo ha hecho, dedique unos minutos a reconocer y apreciar estos esfuerzos y el impacto positivo que tendrán para su organización.

Recuerde que hay dos formas de utilizar el manual de estrategias:

1) Autocompletar y recibir el certificado de finalización: Complete este programa en línea a su propio ritmo, utilizando el manual de estrategias como herramienta para ayudarlo a adoptar políticas clave y desarrollar un plan de continuidad del negocio para recibir un certificado de finalización.

2) Finalización verificada y recepción de la certificación de preparación cibernética de CRI: Complete este programa de preparación cibernética en línea, utilizando el manual de estrategias para adoptar políticas clave, desarrollar un plan de continuidad del negocio, capacitar a sus empleados y enviar una carta de certificación firmada. A continuación, permita que un instructor de ciberseguridad de CRI revise y verifique su manual de estrategias completo.

Si está interesado en obtener la certificación de preparación cibernética de CRI, escriba a info@cyberreadinessinstitute.org. NO envíe este manual de estrategias a CRI por correo electrónico ni mediante ningún otro servicio de transferencia de datos. En lugar de ello, póngase en contacto con nosotros y nos encargaremos de los siguientes pasos para la certificación.