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 plan, 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, LINUX, 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.