Curso Fundamentos de Ciberseguridad

Módulo 4

Relator: José Morales Antúnez

¿Qué es un plan de contingencia?

Un plan de contingencia en ciberseguridad es un documento que establece las medidas y procedimientos necesarios para preparar y responder a incidentes cibernéticos. El objetivo principal de un plan de contingencia en ciberseguridad es minimizar la interrupción de los servicios críticos de la organización y reducir el impacto de los incidentes cibernéticos en la organización y sus clientes.

Un plan de contingencia en ciberseguridad debe incluir información detallada sobre cómo detectar, responder, contener y recuperarse de incidentes cibernéticos, así como sobre cómo comunicar y colaborar con otros departamentos y organizaciones durante un incidente. El plan debe ser revisado y actualizado regularmente para asegurar que esté actualizado con las últimas amenazas y mejores prácticas.

Algunos de los elementos que podrían incluir un plan de contingencia en ciberseguridad:

- Una lista de contactos clave para contactar en caso de incidente
- Una lista de procedimientos para detectar, investigar y contener incidentes
- Una lista de procedimientos para recuperarse de incidentes y restaurar los servicios
- Una lista de procedimientos para comunicar incidentes a los interesados apropiados
- Un plan de comunicación interna y externa
- Un plan de capacitación y sensibilización del personal

En resumen, un plan de contingencia en ciberseguridad es un plan detallado para prepararse y responder a incidentes cibernéticos, con el objetivo de minimizar los daños y continuar con las operaciones de la organización de manera segura.

Otra definición que podríamos mencionar la siguiente es que es un documento en el que se recogen todas las medidas necesarias que debe contemplar una organización para mantener su actividad normal tras sufrir una interrupción no planificada en el servicio. Esta interrupción puede venir motivada por numerosas causas (desastres naturales, accidentes, fallos energéticos, fallos internos o ciberataques).

Este tipo de planes deben revisarse y probarse periódica y generalmente contienen la siguiente información:

- Los tipos de amenazas que pueden afectar al negocio.
- Los casos de uso que provocarían la activación del plan.
- Las piezas claves de la organización (infraestructura TIC, sistemas de comunicación, suministros y equipos, copias de seguridad de datos y sus ubicaciones e, incluso, infraestructuras físicas.
- La identificación de las personas clave en caso de necesitar gestionar una crisis y la asignación de roles y responsabilidades según corresponda, para que todo el mundo tenga claro qué debe hacer y qué se espera de su trabajo.
- Incluye la información de contacto tanto de las personas que ocupan roles esenciales, así como la de los proveedores estratégicos de la organización.

Beneficio de contar con un plan de contingencia

- Poder disponer de una estrategia a corto, medio y largo plazo que contribuya a la protección y continuidad del negocio.
- Conocer cuál es la información más importante para el negocio de la organización: diseños, planos, especificaciones técnicas, clientes, etc.
- Identificar cuáles son las amenazas que pueden tener un impacto significativo en nuestra actividad.
- Determinar los riesgos y poder realizar una gestión adecuada de los mismos.
- Definir planes y medidas de contingencia para limitar el impacto de nuestra organización a imprevistos como incidentes de ciberseguridad.
- Dar un mejor servicio a nuestros clientes al asegurar acuerdos de nivel de servicio y que ello supone una ventaja competitiva a la hora de contratar sus servicios.

No hay un plan de ciberseguridad infalible ni único, del mismo modo que el plan de contingencia tampoco lo será. Cada empresa debe tener su propio plan de ciberseguridad y cada empresa se enfrentará a los problemas de manera diferente a como lo hacen otras.
Lo que es seguro es que el encargado de ciberseguridad debe tenerlo todo presente para evitar males mayores.

Una contingencia se refiere a actividades o eventos que ocurren más allá del rango normal de operaciones organizacionales. Por lo tanto, un plan de contingencia es un plan definido y procesable que se implementará si ocurre un riesgo comercial identificado o un evento desafortunado. Los planes de contingencia son parte de la gestión de riesgos y se pueden crear para riesgos identificados o no identificados. También se pueden crear para aprovechar oportunidades estratégicas.

Un plan de contingencia no es solo una necesidad para las grandes empresas, ya que las pequeñas y medianas empresas también pueden verse afectadas por eventos imprevistos.

También se pueden adaptar a departamentos específicos. Por ejemplo, la necesidad de proteger, restaurar y utilizar datos en una organización puede requerir un plan de contingencia del departamento de servicios de información.

La importancia de los planes de contingencia radica en que permiten que las organizaciones reanuden las funciones comerciales normales lo más rápido posible después de que haya ocurrido un evento imprevisto.

Un buen plan de contingencia debe incluir:

- Desastres naturales como terremotos, incendios y huracanes.
- Crisis, incluidas lesiones y accidentes en el lugar de trabajo.
- Personal como huelgas y muertes de empleados.
- Pérdida de datos.
- Problemas de productos, como reubicaciones de planes.
- Mala gestión, como destrucción accidental y robo.

El proceso de desarrollo de un plan de contingencia implica la identificación de operaciones y sectores comerciales esenciales y la determinación de cómo estos procesos pueden verse afectados

por la ocurrencia de eventos imprevistos. Se deben identificar y documentar las acciones que serían necesarias para devolverlos a sus operaciones normales, incluidos los recursos que se necesitarían para ello. Un buen plan de contingencia incorpora cada área funcional en una organización.

Beneficios de contar con un plan de contingencia

Protección de la información confidencial: Un plan de contingencia de ciberseguridad ayuda a proteger la información confidencial de una organización, como datos de clientes y transacciones financieras, de ser accedidos o modificados por atacantes.

Continuidad del negocio: Un plan de contingencia de ciberseguridad permite a una organización continuar sus operaciones críticas en caso de un evento inesperado, como un ataque cibernético, lo que minimiza el impacto en el negocio.

Reducción de costos: Un plan de contingencia de ciberseguridad ayuda a reducir los costos de respuesta a un incidente, ya que la organización ya ha identificado los riesgos y ha creado procedimientos de respuesta antes de que ocurra el incidente.

Mejora de la reputación: Al tener un plan de contingencia de ciberseguridad, una organización puede demostrar a sus clientes y partes interesadas que está tomando medidas para proteger sus datos y operaciones, lo que puede mejorar su reputación.

Cumplimiento normativo: Algunas regulaciones y estándar de seguridad requieren contar con un plan de contingencia, contar con uno permite cumplir con estas regulaciones y estándares.

¿Por qué realizar un plan de contingencia?

Ejecutar un conjunto de normas, procedimientos y acciones básicas de respuesta que se deben tomar de forma efectiva, adecuada y oportuna, ante una situación excepcional.

Estar preparados. Las empresas han de estar preparadas para proteger a todos los públicos ante una serie de escenarios de riesgos a través de una planificación preventiva y eficiente. Por ejemplo, a través de plataformas que nos permitan estar conectados con todos los niveles de la empresa y tener acceso remoto a aquellos datos que son necesarios para la realización de nuestra labor.

Mejorar la flexibilidad. Cuando se realiza un plan de contingencia las organizaciones obtienen un nivel de flexibilidad que les permite adaptarse a numerosos desafíos que puedan ocurrir en un futuro.

Evitar entrar en pánico. Cuando una empresa no está preparada, todos los públicos se encuentran en una situación de incertidumbre que a su vez provoca una situación de pánico al saber que no hay soluciones preestablecidas. Esto cambia por completo, con los planes de contingencia, en ellos está esclarecido todo lo que deben saber y cómo actuar antes una situación, pudiendo implementar una solución cuando sea necesario.

Reaccionar en un breve periodo de tiempo. Cuando una empresa cuenta con un plan de contingencia elaborado obtiene mayor probabilidad de poder reaccionar en un tiempo menor a situaciones no planificadas.

Eludir una toma de decisiones precipitadas. Normalmente las decisiones tomadas de manera precipitada no suelen ser las correctas por ello debemos evitarlas, siempre y cuando sea posible. Por este motivo, los expertos en negocios diseñan planes de contingencia después de una exhaustiva investigación y observación, obteniendo una serie de pautas a realizar ante diferentes situaciones que puedan ocurrir.

Optimizar los tiempos de tu empresa. Una vez la organización es consciente de los riesgos que puede conllevar una situación excepcional como la actual pandemia COVID-19, el plan de contingencia nos ayudará a minimizar el tiempo de recuperación de los datos (RTO), además del tiempo de improductividad empresarial (RPO).

Maximizar la seguridad en el acceso a tus datos. Hoy en día, las empresas almacenan los datos en la nube por lo que debemos estar preparados y garantizar el acceso a estos en un proceso seguro. Para ello, habrá que confirmar el acceso a dichos datos por las personas responsables de cada organización.
Clasificar los activos de la empresa otorgando prioridad para su protección. No podemos salvaguardar todos los activos de una empresa de la misma forma, es por ello, debemos saber cuáles son aquellos activos con mayor valor y priorizar su seguridad para que toda la organización pueda mantener su labor con la mayor naturalidad posible.
Prevenir y minimizar pérdidas económicas. En una situación anormal, el funcionamiento de una organización se ve afectado en todos los aspectos y por supuesto también en los económicos, es por ello, tener un plan de contingencia establecido permitirá afrontar la situación de la forma que nos permita mantener nuestra actividad laboral.

Para elaborar un plan de contingencia debemos seguir unos pasos fundamentales que nos permita realizarlos de una manera detallada:

- Identificar los escenarios de riesgo en tu empresa.
- Determinar las actividades críticas y prioritarias de la organización e identificar cuándo se podrá reanudarlas.
- Determinar que se necesita para que la organización mantenga su actividad laboral.
- Selecciona al líder o equipo responsable de llevar a cabo el plan.
- Establece las estrategias de protección antes del incidente y las medidas de contingencia.
- Respuesta al incidente: estabilizar la situación, eliminar amenazas y peligros, además de prever daños adicionales o desastres consecuentes.
- Considerar el lugar donde se reanudará la actividad: ¿desde las instalaciones, desde casa, etc.?
- Reservar una cantidad suficiente para soportar los gastos fijos mínimos de un mes.

¿Qué es un BCP?
BCP (Business Continuity Planning) por sus siglas en ingles es un Plan de Continuidad de Negocio, es un proceso de planificación para garantizar que una organización pueda continuar sus operaciones críticas en caso de un evento inesperado, como un desastre natural, un ataque cibernético o un fallo en el sistema. El objetivo de un BCP es minimizar el impacto de un evento en la organización y asegurar que los servicios esenciales sean restaurados lo antes posible. Esto incluye la identificación de riesgos, la creación de procedimientos de respuesta y la implementación de medidas para mitigar el impacto de un evento. En ciberseguridad se enfoca en prevenir, detectar y responder a incidentes de seguridad cibernética, así como en garantizar la continuidad del negocio en caso de un incidente. Esto incluye medidas preventivas, formación de los empleados, implementación de controles de seguridad, planes de respuesta y recuperación en caso de un incidente.

¿Qué es un DRP?
Disaster Recovery Planning (DRP) por sus siglas en ingles Plan de Recuperación ante Desastres, es un proceso de planificación que se enfoca en la recuperación de las operaciones críticas de una empresa después de un desastre, interrupción o incidente de seguridad. En el contexto de la ciberseguridad, el DRP se enfoca en garantizar que una empresa pueda restaurar sus sistemas y datos críticos después de un incidente de seguridad cibernética, como un ataque cibernético o una violación de datos. Esto incluye medidas como la creación de copias de seguridad y la implementación de planes de respuesta y recuperación, así como la identificación de puntos de recuperación y la asignación de responsabilidades para la recuperación.

En el DRP se definen los procedimientos y medidas necesarias para recuperar un sistema informático después de un incidente de seguridad, como un ataque cibernético, una interrupción en el suministro eléctrico o un desastre natural. El objetivo principal de DRP es minimizar los tiempos de inactividad y asegurar que los servicios críticos se restablezcan lo antes posible.
El DRP también implica la identificación de los activos críticos y la evaluación de los riesgos y las vulnerabilidades. Esto es importante para poder priorizar los esfuerzos de recuperación y asegurar que los servicios críticos se restablezcan primero.

Beneficios de implementar un BCP y DRP correctamente en una empresa.
Hay varios beneficios para una empresa que implementa un plan de Business Continuity Planning (BCP) y Disaster Recovery Planning (DRP):

- Reducción del riesgo: Al planificar y prepararse para incidentes, una empresa puede reducir el riesgo de interrupciones en sus operaciones y minimizar los daños causados por un incidente.
- Continuidad del negocio: Un BCP y DRP bien implementado garantizará que una empresa pueda continuar sus operaciones críticas en caso de un incidente, lo que ayudará a proteger la reputación y los ingresos de la empresa.
- Mejora de la resiliencia: Al tener un plan de respuesta y recuperación en su lugar, una empresa estará mejor preparada para manejar incidentes y se recuperará más rápidamente.
- Mayor confianza de los clientes: Una empresa que ha implementado un BCP y un DRP puede mostrar a sus clientes y proveedores que está comprometida con la continuidad del negocio y la seguridad de sus datos, lo que puede aumentar la confianza de estos en la empresa.
- Cumplimiento normativo: Muchas normas y regulaciones, como la norma ISO 22301, requieren un BCP y un DRP, al cumplir con estas normas se evita sanciones y multas.
- Mejora de la eficiencia: La planificación y la preparación para incidentes pueden ayudar a una empresa a identificar y eliminar cuellos de botella innecesarios en sus operaciones, lo que puede mejorar la eficiencia general de la empresa.

Diferencia entre DRP y BCP
El plan de recuperación ante desastres es una parte del plan de continuidad de negocio.
Está relacionado con el área de TI y se refiere a las acciones que se van a emprender para resolver cualquier eventualidad que impida que el personal pueda acceder al sistema, ya sea un desastre natural, un ataque informático o una contingencia.
El DRP también contempla establecer el tiempo objetivo de recuperación (RTO), que es el periodo máximo que puede tardar el negocio en reanudar operaciones; y el punto objetivo de recuperación (RPO), es decir, el punto máximo de datos que se pueden perder en el evento sin comprometer el resto de la información.
Por su parte, el plan de continuidad de negocio establece toda la estrategia para hacer frente a una eventualidad, no solo ante un evento repentino.
Por ejemplo, también puede abarcar el plan de gestión de incidentes (incident management plan o IMP), que contempla algún incidente de seguridad, sin que haya una interrupción total de la operación o una gran pérdida de datos.

¿Qué es la ISO 22301?
La norma ISO 22301 es un estándar internacional para la gestión de continuidad del negocio. Es una norma para desarrollar, implementar, mantener y mejorar un sistema de gestión de continuidad del negocio (BCMS, por sus siglas en inglés) en una organización. La norma establece los requisitos para

establecer, implementar, mantener y mejorar un sistema de gestión de continuidad del negocio que permita a la organización responder a incidentes y recuperarse en un tiempo razonable.
La norma se centra en la gestión de riesgos, la continuidad del negocio y la recuperación de incidentes, y proporciona un marco para desarrollar un plan de continuidad del negocio que sea efectivo y eficiente. El objetivo es garantizar que una organización pueda continuar sus operaciones críticas y proteger su reputación y su rentabilidad en caso de un incidente.

La norma ISO 22301 contiene los siguientes elementos clave:

- Alcance: describe el alcance del sistema de gestión de continuidad del negocio y los requisitos de la norma.
- Terminología: define términos y definiciones esenciales utilizados en la norma.
- Contexto de la organización: describe cómo la organización debe considerar su entorno interno y externo y cómo puede afectar a su capacidad para continuar sus operaciones críticas.
- Liderazgo y compromiso: establece la importancia de la liderazgo y compromiso en la implementación y mantenimiento de un sistema de gestión de continuidad del negocio.
- Planificación: proporciona un marco para la planificación de la continuidad del negocio, incluyendo la identificación de activos críticos, la evaluación de riesgos y la elaboración de planes de contingencia.
- Implementación y operación: describe cómo implementar y operar el sistema de gestión de continuidad del negocio, incluyendo la asignación de responsabilidades, la comunicación y la documentación.
- Revisión por la dirección: establece la importancia de la revisión y evaluación continua del sistema de gestión de continuidad del negocio por parte de la dirección.
- Mejora: proporciona un marco para la mejora continua del sistema de gestión de continuidad del negocio.

La norma ISO 22301 es una norma completa y debe ser implementada de manera adecuada para cumplir con los requisitos de continuidad del negocio.
La implementación de la norma ISO 22301 puede proporcionar varios beneficios para una organización, algunos de ellos son:

- Mejora de la resiliencia: al establecer un sistema de gestión de continuidad del negocio, una organización puede mejorar su capacidad para continuar sus operaciones críticas en caso de una interrupción.
- Reducción de riesgos: al identificar y evaluar los riesgos y desarrollar planes de contingencia, una organización puede reducir el impacto de un incidente en sus operaciones.
- Aumento de la confianza: al demostrar su compromiso con la continuidad del negocio, una organización puede aumentar la confianza de sus clientes, proveedores y otros interesados.
- Mejora de la eficiencia: al establecer procesos y procedimientos claros para la continuidad del negocio, una organización puede mejorar su eficiencia y reducir los costos.
- Mejora de la reputación: al cumplir con un estándar internacionalmente reconocido, una organización puede mejorar su reputación y posicionamiento en el mercado.
- Mejora de la competitividad: al cumplir con los requisitos de la norma ISO 22301, una organización puede mejorar su competitividad y diferenciarse de sus competidores.
- Mayor seguridad para los colaboradores: al tener un plan de contingencia, se garantiza una mayor seguridad para los colaboradores de la organización en caso de un incidente.

La implementación de la norma ISO 22301 puede ser un proceso complejo, pero se puede dividir en los siguientes pasos:

- Comprender los requisitos de la norma: leer y comprender los requisitos de la norma es esencial para implementar un sistema de gestión de continuidad del negocio eficaz.
- Realizar un análisis de riesgos: identificar y evaluar los riesgos que pueden afectar a las operaciones críticas de la organización es esencial para planificar la continuidad del negocio.
- Establecer objetivos y metas: establecer objetivos y metas claros para la continuidad del negocio ayudará a la organización a medir su progreso y asegurar que se cumplan los requisitos de la norma.
- Desarrollar un plan de continuidad del negocio: una vez identificados los riesgos y establecidos los objetivos, se debe desarrollar un plan de continuidad del negocio que incluya planes de contingencia y procedimientos para la recuperación.
- Implementar y mantener el sistema: implementar y mantener el sistema de gestión de continuidad del negocio es esencial para asegurar que la organización pueda continuar sus operaciones críticas en caso de una interrupción.
- Evaluar y mejorar continuamente: es necesario evaluar y mejorar continuamente el sistema de gestión de continuidad del negocio para asegurar que sigue siendo eficaz y cumpliendo con los requisitos de la norma.
- Certificar el sistema: Una vez implementado y evaluado el sistema, se puede solicitar una certificación para la norma ISO 22301 con un organismo acreditado para verificar que se cumplen los requisitos de la norma.
- Es importante tener en cuenta que la implementación de la norma ISO 22301 debe ser un proceso continuo y debe involucrar a toda la organización, no solo a un departamento o un grupo específico.

Implementación plan de contingencia.

La implementación de un plan de contingencia es el proceso de establecer medidas para prepararse y responder a eventos imprevistos o desastres. Esto incluye la identificación de riesgos potenciales, la creación de procedimientos para responder a estos eventos y la asignación de responsabilidades a individuos o equipos específicos.

Para implementar un plan de contingencia, se deben seguir los siguientes pasos:

- Identificar los riesgos potenciales: Esto incluye la evaluación de los riesgos naturales, tecnológicos y humanos que pueden afectar a su organización.
- Crear procedimientos de respuesta: Establezca los procedimientos que se seguirán en caso de un evento de emergencia, incluyendo la comunicación, la evacuación y la recuperación.
- Asignar responsabilidades: Asigne responsabilidades específicas a individuos o equipos para asegurar que todos sepan qué hacer en caso de un evento de emergencia.
- Capacitar al personal: Asegúrese de que todos los empleados sepan cómo responder y qué hacer en caso de un evento de emergencia.
- Pruebas y simulacros: Realice simulacros y pruebas regulares para evaluar la eficacia de su plan de contingencia y hacer ajustes necesarios.
- Mantenimiento y actualizaciones: Revisa y actualiza regularmente el plan de contingencia para asegurar que está actualizado y sigue siendo relevante.

Plan de contingencia sobre riesgos de seguridad de la información en una empresa contable

ANÁLISIS DE SU IMPACTO

Una violación a la seguridad de los sistemas informáticos sería un problema técnico, de servicio al cliente, de confidencialidad y de relaciones públicas.

MEDIDAS A TOMAR

Buscar las infiltraciones, contactar a la clientela para dar aviso y reforzar la seguridad durante el evento.

RECURSOS PARA IMPLEMENTAR LAS MEDIDAS

Ayuda técnica, acceso máximo al servidor, protocolos de atención y agentes con máxima disponibilidad.

PROTOCOLOS Y RESPONSABLES

Corresponden a las áreas de ingeniería, administración web, atención y gestión de redes sociales.

TRANSICIÓN A LA NORMALIDAD

Analizar el impacto del evento, reforzar los protocolos de seguridad y mejorar el plan de actuación.

Plan de contingencia sobre cambio de modalidad de trabajo en una maquiladora

ANÁLISIS DE SU IMPACTO

Si es necesario que la fábrica opere con solo el 50 % de su personal, esto impactará en la productividad y finanzas de la empresa, así como en su supervivencia.

MEDIDAS A TOMAR

Establecer quiénes pueden realizar sus labores de forma remota y cómo organizar al personal presencial.

RECURSOS PARA IMPLEMENTAR LAS MEDIDAS

Acondicionamiento del espacio físico y envío de equipo y recursos a los colaboradores remotos.

PROTOCOLOS Y RESPONSABLES

Líderes y empleados delegados para labores de organización y supervisión de las medidas sanitarias.

TRANSICIÓN A LA NORMALIDAD

Automatizar actividades en la medida de lo posible y flexibilizar los modos de trabajo (sobre todo del personal administrativo).

Plan de contingencia sobre la pérdida de clientes en una empresa informática

ANÁLISIS DE SU IMPACTO

Una empresa informática que enfrenta una gran pérdida de clientes debido a la competencia tendrá un problema financiero y de posicionamiento en el mercado.

MEDIDAS A TOMAR

Mejorar el producto y sus funciones o lanzar precios de promoción.

RECURSOS PARA IMPLEMENTAR LAS MEDIDAS

Fondos de ahorro para solventar gastos corrientes e invertir en desarrollo de producto.

PROTOCOLOS Y RESPONSABLES

Departamentos de desarrollo, marketing y ventas.

TRANSICIÓN A LA NORMALIDAD

Monitorear el mercado y realizar mejoras constantes al producto.

HubSpot