Guía

Ejercicio de la Unidad de Crisis Ciberataque

controllit
Business Continuity Management

Contenido

Introducción

Titulares como "Ciberdelincuencia", "Se filtran 2 millones de datos de clientes", "Un ataque de hackers paraliza la empresa durante semanas" se publican repetidamente en los medios de comunicación. A pesar de todas las medidas de mitigación de riesgos y las precauciones de la empresa, este escenario también se produce en Alemania varias veces al año, con daños millonarios.

¿Está su empresa preparada para este escenario?

Dans ce guide sur la cyberattaque lors d'un exercice de cellule de crise, nous souhaitons présenter les thèmes essentiels à la bonne gestion d'une telle crise.
Ce faisant, nous accordons une attention particulière aux objectifs classiques de la gestion de crise :

- **Protección de la vida humana**/daño a las personas y al medio ambiente
- **Limitación de daños Evitar**/minimizar los daños económicos, evitar los daños a la imagen, salvaguardar los pro-cesos empresariales críticos (en términos de tiempo)
- **Protección del funcionamiento normal** de las partes no afectadas de la planta

Otro punto de interés es la cooperación eficaz y eficiente de los miembros de su equipo de crisis (KS) sobre la base de las **tareas básicas de un equipo de crisis**:

- Identificación y análisis de situaciones de crisis
- Definición de una estrategia de gestión de crisis
- Desarrollo de opciones de actuación
- Evaluación de las perspectivas de éxito, los riesgos y las oportunidades
- Priorización y toma de decisiones
- Informar sobre las medidas adoptadas
- Delegación y control de las acciones
- Evaluación y reevaluación

Medidas preventivas

La gestión de crisis es un proceso reactivo, pero por supuesto también hay que preparar a la organización de gestión de crisis para sus tareas con medidas preventivas.

Aquí resumimos las medidas clave con una perspectiva en el escenario del "ciberataque":

Compruebe si todos los miembros responsables de su organización de crisis son paces de actuar y están preparados para ello por ejemplo, mediante formación periódica, estructura de reuniones, intercambio periódico de información, medidas de sensibilización):

- Miembros de la unidad de crisis, incluidos sus suplentes
- Participantes a nivel táctico (jefes de departamento, etc.)
- Ejecutores a nivel operativo (empleados de los departamentos especializados)

Aproveche su sistema de gestión de la continuidad del negocio (BCM) cuando lo haya implantado:

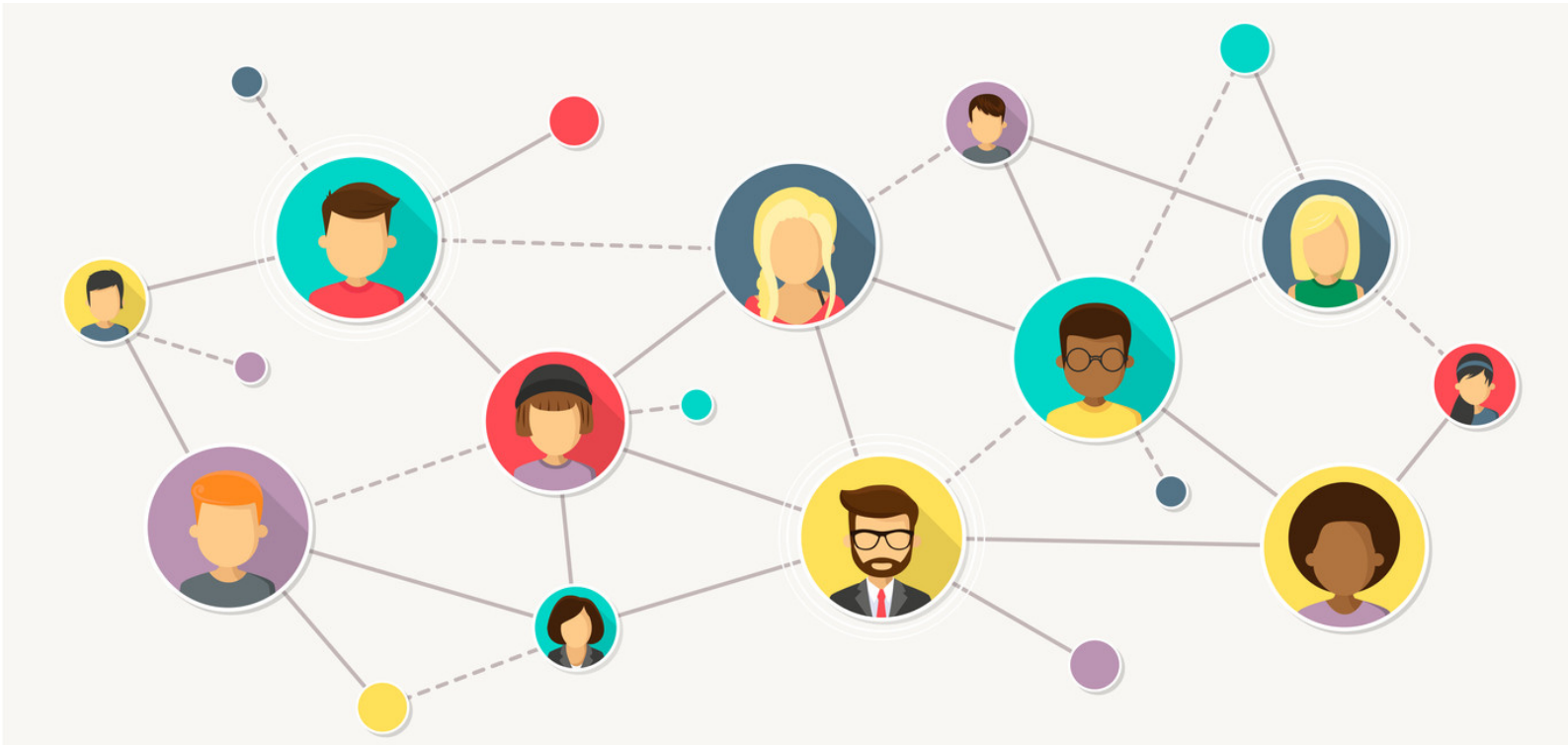
- Revisar la oportunidad y la eficacia de los planes de continuidad de la actividad para el escenario de fallo informático:
  - → En caso de fallo informático, ¿las opciones de solución utilizadas son capaces de compensar temporalmente un fallo del proceso de negocio (especialmente en lo que respecta a las soluciones alternativas implementadas)?
  - → ¿Son efectivas y aplicables sus medidas de respaldo, como el paso de caliente a frío, etc.?
- Si no ha implantado un Système de gestion de la continuité des activités (BCMS), compruebe su capacidad operativa sobre la base de los siguientes temas

Aproveche su Sistema de Gestión de la Continuidad del Servicio de TI (ITSCM) y su Sistema de Gestión de la Seguridad de la Información (ISMS) cuando los implemente:

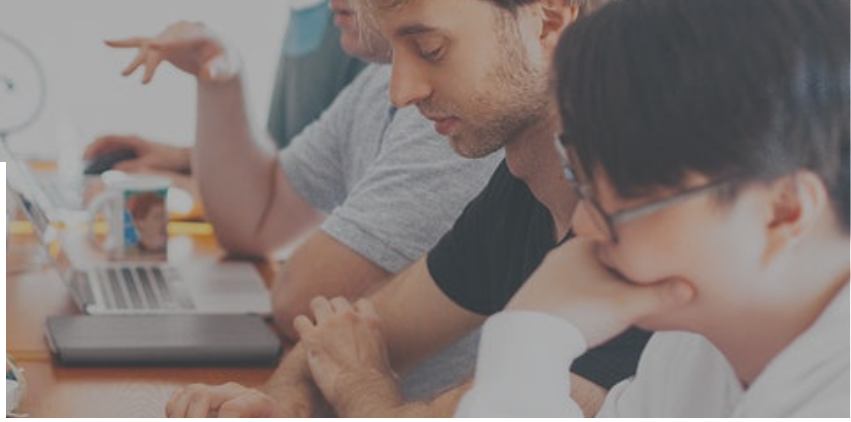
- En caso de fallo informático, ¿las opciones de solución utilizadas son capaces de compensar temporalmente un fallo del proceso de negocio?
- ¿Pueden cumplirse sus valores objetivo de TI, como el tiempo de recuperación real (RTA) y el punto de recuperación real (RPA)?
- ¿Está la disponibilidad de los servicios informáticos suficientemente garantizada desde el punto de vista del ITSCM?
- ¿Se garantiza adecuadamente la recuperación de recursos en caso de ataque en el ITSCM?
- ¿Se salvaguardan adecuadamente los objetivos de protección del mecanismo de apoyo institucional?
- Si no ha implantado ITSCM y/o ISM, compruebe si está preparado con los temas que se indican a continuación

Medidas preventivas

Utilizar el establecimiento y mantenimiento por parte del gestor de crisis de interfaces externas (en este caso, en particular, autoridades como la Oficina Estatal de Policía Criminal, Autoridad Federal de Supervisión Financiera, etc.)



Crear comprensión y concienciación, así como seguridad procedimental para el tema (medidas de concienciación



Medidas reactivas

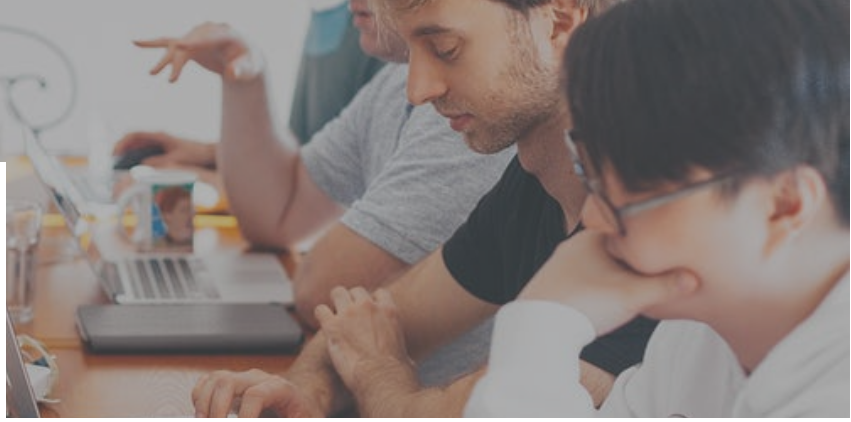
En un ejercicio de gestión de crisis (pero también en el caso de que se produzca realmente el incidente), las medidas de reacción en caso de incidente están en primer plano. Esto implica un comienzo ordenado del trabajo de su equipo de crisis apoyado por una visión general de los temas. A continuación se presentan los primeros pasos, así como los puntos detallados para los miembros individuales del equipo de crisis.

Visión general de los temas

En caso de ciberataque, las medidas iniciales se ponen en marcha con la participación de la ITSCM/ISM y, si es necesario, con la participación de las autoridades externas: La atención se centra inmediatamente en la limitación de los daños y en las medidas de seguridad.

Además, las siguientes medidas y consideraciones son esenciales:

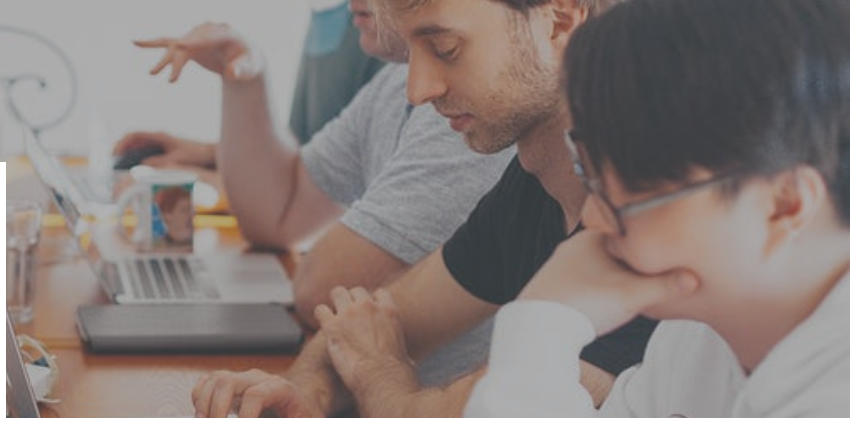
- Tenga en cuenta los siguientes puntos a la hora de alertar y constituir el equipo de crisis:
  - → ¿Sala de personal de crisis utilizable (posiblemente uso de sala de KS alternativa)?
    - ¿Puede su sala de crisis utilizarse de forma autosuficiente con respecto a los componentes informáticos individuales o varios?
    - Las herramientas virtuales con conexión al sistema de la empresa probablemente no están disponibles
  - → Identificación de los sistemas y programas informáticos disponibles (desde el teléfono hasta el sitio web, pasando por los ordenadores portátiles de emergencia)
  - → Comunicación rápida interna y externa
    - Primera información: Confirmación del acontecimiento sobre la base de una redacción predefinida (idealmente en diez minutos)
    - Hay que prestar especial atención al posicionamiento de la empresa y a la estrategia de comunicación externa (responsabilidad, autor/víctima, etc.)
  - → Identificación y delimitación del alcance actual y potencial de los daños (interfaz ITSCM/IT)
  - → Activación de los BCP y del plan de recuperación de TI (si está disponible)
  - → Obtener la aprobación del presupuesto (si es necesario)



Medidas reactivas

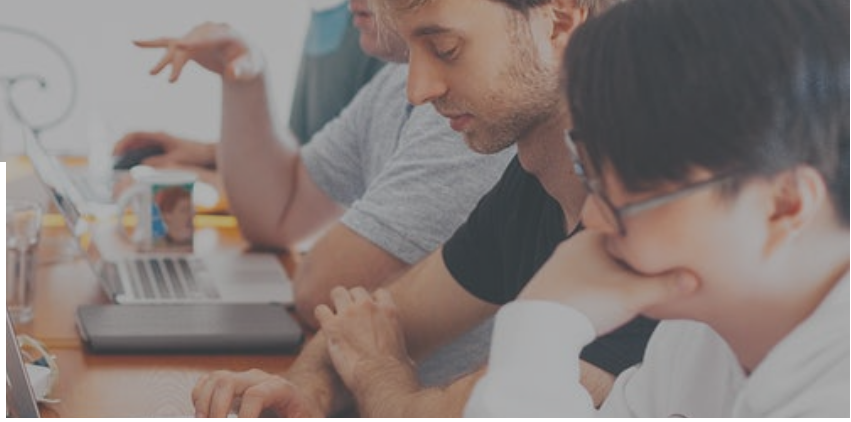
- Obsérvese una cascada dinámica de impactos (esto es bastante probable): Suele producirse un efecto dominó dentro de los sistemas informáticos
- Obsérvese el altísimo impulso inicial y la probable presión (debido a la alta dependencia general de las TI) de la fase de caos, especialmente en lo que respecta a la información (abundancia y escasez)
- Realizar las tareas básicas de inicialización y asegurar las operaciones de emergencia
- Utilice su forma de organización: ¿Existe un equipo de asistencia y servicio (AST), un equipo de comunicación o los miembros del equipo de crisis son responsables de la conexión estructurada de los departamentos ?
  - → ¿Cuáles son los canales de notificación e información?
  - → ¿Cómo se integran los representantes de la interfaz BCM, ITSCM e ISM en el unidad de crisis?
- Utilice la conexión de los departamentos especializados con el Equipo de asistencia y servicio (AST) o la unidad de crisis para determinar la situación: :
  - → ¿Qué departamentos se ven afectados?
  - → ¿Qué departamentos son capaces de trabajar/no son capaces de trabajar?
  - → ¿Qué servicios informáticos se ven afectados?
  - → ¿Qué servicios informáticos se pueden utilizar?
  - → ¿Se ven afectados los datos de los empleados y/o de los clientes?
  - → ¿Qué salvaguardias tienen éxito/pueden ser prioritarias?

- Garantizar el flujo de información y la conexión coordinada con interfaces externas (por ejemplo, autoridades como la Oficina Nacional de Policía Criminal, etc.), así como el cumplimiento puntual de las obligaciones de información:
  - → Si es necesario, integración de la Oficina Nacional de Policía Criminal o de expertos externos (por ejemplo, expertos en informática) en el equipo de crisis
  - → Cumplimiento de los plazos de información de acuerdo con los requisitos de la empresa y del sector



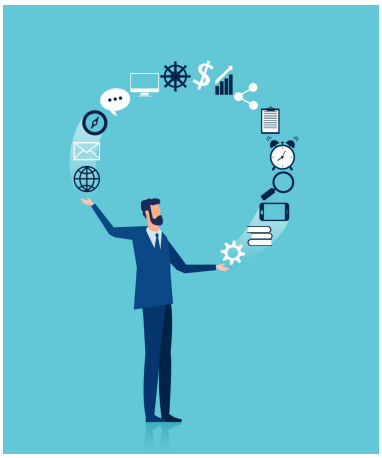
Medidas reactivas

- Controlar el conocimiento avanzado de la situación: ¡utilizar la visualización para tener una visión general!
  - → Alcance interno y externo de los daños: ¿Qué servicios informáticos se ven afectados? ¿Qué RTA y RPA son actualmente realistas? ¿Qué datos están afectados?
  - → ¿Qué departamentos se ven afectados? En particular: ¿Qué procesos empresariales de tiempo crítico y qué RTO existen?
  - → ¿Qué departamentos son viables/no viables? ¿Existen opciones de recuperación del negocio?
  - → ¿Qué servicios informáticos son necesarios en una operación de emergencia y son utilizables/recuperables? ¿Prioridad en la línea de tiempo?
  - → Responsabilidad del suceso: culpa propia/culpa externa/cumplimiento del deber de diligencia
  - → Resumen de medidas y control de estado
  - → Determinación de la causa raíz para la limitación optimizada de los daños (por ejemplo, a través del análisis forense de TI)
- Utilice sus umbrales!
  - → ¿Se han definido los umbrales y qué umbrales se han superado? Umbral potencialmente superado para:
    - Fallo informático
    - Fallo del proveedor de servicios informáticos
    - Si procede, valores umbral ITSCM (si está disponible)
- Tenga en cuenta las implicaciones para la oficina en casa y el trabajo a distancia
  - → Las conexiones VPN también pueden tener un impacto en los dispositivos privados de los empleados (bring-your-own-device).
- Evalúe las perspectivas de su equipo de crisis
  - → En caso de fallo informático, es probable que el equipo de crisisse utilice durante un periodo de tiempo más largo (dependiendo del tipo y la gestión del ciberataque)
- Inicie el proceso de recuperación en paralelo con la operación de emergencia (recuperación informática)
- Compruebe la cobertura de su seguro y las obligaciones de notificación (por ejemplo, el seguro de interrupción de la actividad empresarial).
- Preste especial atención al apoyo de las líneas de atención telefónica
  - → Si la telefonía sigue funcionando, cabe esperar un gran volumen adicional (consultas de clientes y medios de comunicación)



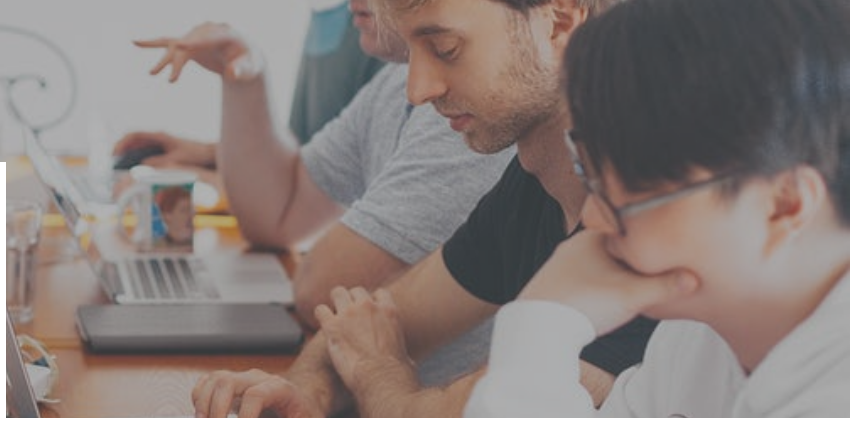
Medidas reactivas

Tareas específicas de los miembros de la unidad de crisis



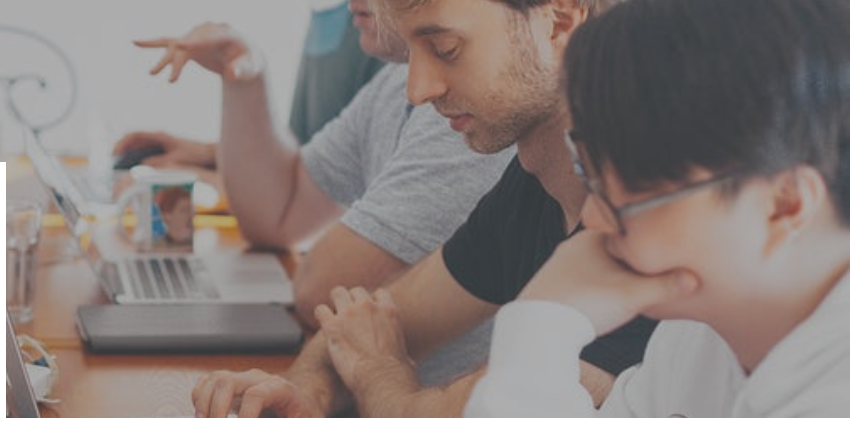
Algunos miembros de su equipo de crisis pueden procesar sus tareas según la lista de com-probación en el escenario de "ciberataque" (por ejemplo, los titulares de funciones de mod-eración, gestión del libro de registro, visualización, asistencia, jurídica y financiera). A contin-uación, se presentan las características especiales de los titulares de funciones con una perspectiva en el escenario de "ciberataque":

- **Líder del equipo de crisis:**
  - → Garantizar la capacidad de trabajo de la unidad de crisis (inicial y regular)
    - Integración de las funciones y papeles pertinentes
    - Disponibilidad de recursos suficientes (técnicos, espaciales, etc.)
  - → Establecer un marco de cooperación que funcione
    - Calendario, sesiones informativas, documentación
  - → Observar las obligaciones de información en el contexto de la empresa (si es necesario, cooperar con el departamento jurídico)
  - → Gestionar activamente la cooperación con las autoridades (si es necesario, integración de los empleados de la Oficina Nacional de Policía Criminal, informática forense)
    - Integración de miembros de las autoridades en el equipo de crisis (¡si es posible!)
  - → En caso necesario y con limitaciones operativas: consolidar la priorización a las operaciones y a las partes interesadas
    - Procesos principales de la empresa/de la empresa
    - ¿Qué es posible con qué medios (palabra clave disponibilidad de TI)?
  - → Comprobar el uso sensato de expertos y proveedores de servicios
  - → Proporcionar información proactiva a la dirección/autoridad decisoria (DMA) y a los comités.
    - Coordinación de la información antes de las comparecencias de prensa (en colaboración con el responsable de comunicación)
  - → Observar el cumplimiento del FORDEC
  - → Asegúrese de llevar a cabo el control de la acción y una comprobación de la efi-cacia
  - → Vigilar el presupuesto y el control financiero
  - → Gestionar activamente la información
  - → Practicar el cuidado activo (este escenario también puede ser estresante)



Medidas reactivas

- **Área de responsabilidad Comunicación:**
  - → Comprobar qué medios de comunicación están disponibles en la situación actual (inicial y en el transcurso de la crisis)
    - Utilizar los medios de comunicación disponibles (internos, externos, redes sociales)
    - Utiliza tus proveedores de servicios para la comunicación si es necesario
  - → Preste atención a la coherencia y fiabilidad de su comunicación externa e interna
    - Primera información: Confirmación del evento a partir de una redacción predefinida (idealmente en los primeros diez minutos).
    - Estrategia de comunicación adecuada (autor/víctima, responsabilidad, apertura, etc.)
    - Extensión rápida de la comunicación a todas las partes interesadas
    - Coordinación dentro del equipo de crisis, especialmente con el departamento de informática, en relación con los plazos previstos (gestión activa de las expectativas internas/externas)
  - → Obsérvese el gran interés por la rendición de cuentas del evento
  - → Utilizar y crear preguntas frecuentes (para necesidades internas y externas)
    - Operar la gestión activa de la información con las interfaces pertinentes
  - → Ayude a sus líneas de atención telefónica (y a los proveedores de servicios, si procede) con plantillas de redacción para garantizar la coherencia de las comunicaciones externas



Medidas reactivas

- **Área de responsabilidad de Recursos Humanos (RRHH) :**
  - → Coordinar las posibles carencias y excedentes de personal (dotación de personal flexible):
    - ¿Qué departamentos tienen necesidades de personal?
    - ¿Qué departamentos pueden proporcionar personal?
    - ¿Qué habilidades tienen/necesitan los empleados (gestión activa de habilidades)?
  - → Coordinar el control de los datos y los derechos de acceso
  - → Garantizar que los expedientes del personal estén a disposición de la equipo de crisis si es necesario y que, en caso contrario, estén cerrados (por ejemplo, para los infractores internos).
  - → Coordinar la gestión de la información sobre el comité de empresa/comité de personal
  - → Asesorar sobre las horas extraordinarias y la legislación laboral si es necesario (las soluciones manuales para las interrupciones de las TI suelen requerir más tiempo y personal)
  - → Comprobar las obligaciones de pago
  - → Utilice los recursos de sus proveedores de servicios
  - → Coordinar las solicitudes de servicios de personal según sea necesario
  - → Gestionar activamente la información
- **Área de responsabilidad de TI :**
  - → Informe a sus proveedores de servicios (incluidos los centros de datos)
  - → Aclarar las responsabilidades dentro de TI
    - Utilización del manual de emergencias informáticas
  - → Investigue y proporcione una estimación del alcance del fallo informático (véase más arriba el alcance de los daños).
  - → Desarrollar una previsión de la propagación de los daños
  - → Mostrar las opciones de los plazos de TI y la recuperación
    - Propuestas de priorización por parte de TI
    - Tenga en cuenta la priorización por parte de la KS
    - Observar las prioridades de la BCM/ITSCM
    - Integrar los aspectos temporales y económicos (viabilidad)
  - → Iniciar la iniciativa de aplicación para restablecer los servicios informáticos
  - → Identificar y coordinar a los proveedores/expertos de servicios informáticos razonables (incluidos los forenses informáticos)
    - para la operación de emergencia
    - para la recuperación
  - → Gestionar la interfaz activa con el ISM, los responsables de la protección de datos
  - → Gestionar activamente la información

Medidas reactivas

- **Área de responsabilidad Departamento**
  - → Compruebe el alcance de los daños en su zona
  - → Consolidar y comunicar los requisitos en su área (en lo que respecta a las tecnologías de la información y al personal adicional si es necesario)
  - → Revise y utilice sus prioridades en relación con las tareas principales
  - → Utilizar y probar la funcionalidad y eficacia de sus medidas de enlace
  - → Utilizar su experiencia para aplicar de forma flexible y creativa las opciones de solución
  - → Gestionar activamente la información
    - Dirección unidad de crisis
    - Cooperación con otros departamentos
- **Área de responsabilidad ISM y protección de datos:**
  - → Comprobar si los objetivos de protección del ISM están afectados
  - → Comprobar la eficacia de las medidas ISM y adaptarlas en función de las necesidades y en cumplimiento de la ley
  - → Cumplir con los requisitos de información en su área de responsabilidad y gestionar activamente la información con las autoridades pertinentes.
  - → Gestionar activamente las interfaces con ITSCM, BCM y los responsables de la protección de datos
  - → Gestionar activamente la información
    - incl. equipo de crisis de consulta sobre todos los temas de ISM y protección de datos

Vuelta a la normalidad y seguimiento

La vuelta a la normalidad tras el despliegue activo de la unidad de crisis requerirá las medidas habituales previstas:

- **Garantizar el retorno al funcionamiento normal de acuerdo con su proceso de recuperación**
  - → Garantizar la funcionalidad básica de los servicios informáticos
    - Organización de los servicios informáticos asegurados y tal vez aún no disponibles en su totalidad (por ejemplo, en lo que respecta al rendimiento, la función y las restricciones de los usuarios)
  - → Coordinación del traspaso de los paquetes de trabajo a los departamentos especializados
  - → Organización del tratamiento de los atrasos
  - → Finalización ordenada del trabajo de la unidad de crisis (incluyendo el traspaso, las líneas de información, la salvaguarda de documentos y registros)

- **Garantizar el seguimiento estructurado o la reevaluación de los acontecimientos (proceso de lecciones aprendidas/análisis post-mortem)**

Controllit AG
Kühnehöfe 20
22761 Hamburg
Alemania
www.controll-it.de

Estado: octubre de 2021

Controllit AG es su socio para la Gestión de Continuidad de Negocio (GCM) - Desde nuestra fundación hemos estado desarrollando conceptos y productos integradores para la Gestión de Continuidad de Negocio, Gestión de Continuidad de Servicios de TI y Gestión de Crisis. Le ayudamos con conceptos estratégicos, organizativos y técnicos para asegurar sus procesos de negocio contra las amenazas y para prever las emergencias.

El contenido de este documento es de carácter informativo para este escenario y la pandemia que en él se describe. Es posible realizar cambios posteriores. Controllit AG no puede garantizar la exactitud de parte de la información proporcionada.

Créditos de las fotos: S. 4: iStock.com/alphaspirit; S. 5: iStock.com/alphaspirit; iStock.com/Maike Hildebrandt; iStock.com/tudmeak; S. 7: iStock.com/SurfUpVector; S. 9: iStock.com/Feodora Chiosea; S. 10: iStock.com/ipuwadol