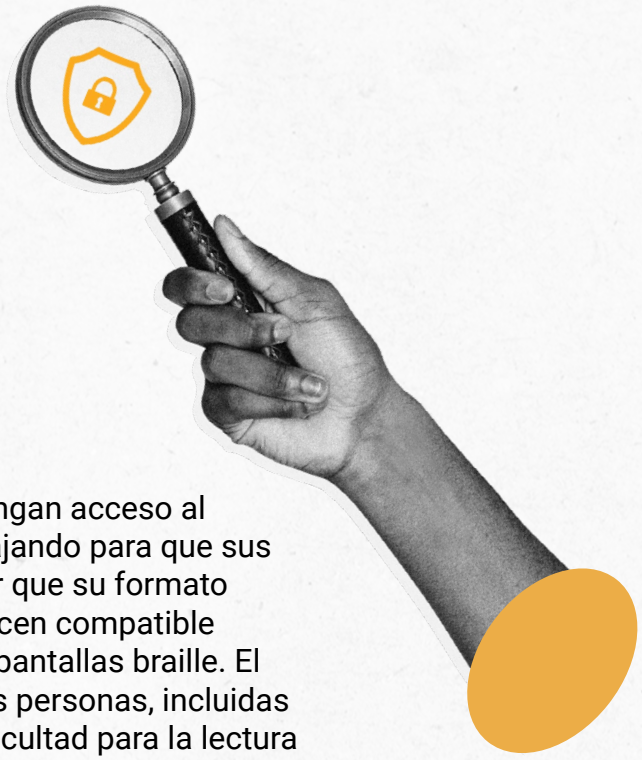
CONSIDERACIONES

PARA EL DISEÑO DE UN PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

20 años Fundación Karisma

KARISMA.ORG.CO

20 años Fundación Karisma



En un esfuerzo para que todas las personas tengan acceso al conocimiento, la Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.

Este informe está disponible bajo Licencia Creative Commons Reconocimiento compartir igual 4.0. Usted puede remezclar, transformar y crear a partir de esta obra, incluso con fines comerciales, siempre y cuando le dé crédito al autor y licencie nuevas creaciones bajo las mismas condiciones.
Para ver una copia de esta licencia visite:

https://creativecommons.org/licenses/by/4.0/deed.es

CONSIDERACIONES PARA EL DISEÑO DE UN PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

El Estado colombiano no ha sido ajeno al aumento de ciberataques en todo el mundo. Los casos con más impacto en el país son los que han sufrido entidades públicas o empresas que prestan servicios a la ciudadanía o al Estado como el Departamento Nacional de Planeación (DANE), el Invima, Keralty (que incluye los servicios de la EPS Sanitas y los de medicina prepagada de Colsanitas y Medisanitas), las Empresas Públicas de Medellín (EPM) o el de IFX Networks (un proveedor de servicios de internet), que por lo menos comprometió el servicio de 50 entidades públicas.

Así mismo, la respuesta que ha dado el Estado a estos ciberataques ha tenido diferentes niveles de efectividad y transparencia. Siendo el caso de IFX Networks el que contó con una respuesta más efectiva y organizada del Estado y en el que más información pública sobre el ciberataque fue liberada.

Desde Fundación Karisma hemos hecho una investigación sobre la forma en que el Estado responde a los incidentes de seguridad digital con la finalidad de entregar algunas recomendaciones y compartir aprendizajes de lo ocurrido. Esperamos que este insumo, creado a partir de la recolección de información en medios de comunicación, solicitudes de información pública, entrevistas con funcionarios públicos y revisión de bibliografía, ayude al Estado a consolidar una política pública en materia de ciberseguridad que lleve a la construcción de protocolos para garantizar los derechos de la ciudadanía en estas circunstancias. Esta no es una guía de respuesta a incidentes, sino una lista de recomendaciones para entidades públicas sobre qué deben tener en cuenta al diseñar sus políticas de seguridad digital.

Queremos compartir algunos insumos adicionales que creemos pueden ser de especial utilidad para los equipos de respuesta y a las directivas de las entidades estatales:

- Las recomendaciones e informes del Grupo de Emergencias Cibernéticas de Colombia -COLCERT- sobre ciberseguridad y respuesta a incidentes.
- Las diez normas no vinculantes sobre comportamiento en el ciberespacio de la Organización de las Naciones Unidas (ONU).
- La caja de herramientas para cibernormas inclusivas de Global Partners Digital.
- Las diez consideraciones para la respuesta a ciber incidentes del Open Web Application Security Project.
- Nuestro informe Ciberataque a Sanitas: impactos diferenciales sobre mujeres cuidadoras paralelo sobre las afectaciones de los ciberataques a grupos especialmente vulnerables.
- El Manual de Ginebra sobre el comportamiento responsable en el ciberespacio creado por DiploFoundation.
- El Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género: Revisión de literatura, Normativas, reglas y directrices y la Herramienta de evaluación de la Asociación para el progreso de las comunicaciones.
- El documento de la Organización de los Estados Americanos (OEA): Guía práctica para CSIRTs.

1. La planeación de la institución debe incluir componentes de ciberseguridad

La respuesta efectiva a incidentes de ciberseguridad requiere planeación previa que minimice tanto la posibilidad de ocurrencia de incidentes, como los efectos adversos relacionados con su mitigación. En todos los casos la respuesta debe estar basada en una evaluación concienzuda de los riesgos identificados en una organización.

Este plan se debe retroalimentar y actualizar de acuerdo con las particularidades y cambios del contexto, la experiencia adquirida en la atención de incidentes pasados y a constantes pruebas que confirmen la efectividad del plan de atención a incidentes. Por tanto, un plan de respuesta a incidentes de ciberseguridad debe incluir acciones previas de preparación, otras que se activan durante el incidente y las que se aplicarán de forma posterior.

Algunos de los elementos que se deben evaluar en la etapa de planeación son:

- Presupuesto para respuesta a incidentes. Se deben evaluar los gastos incluídos, el licenciamiento de herramientas de seguridad digital y las capacitaciones a funcionarios y directivas. Dado que los ciberataques afectan a la ciudadanía se debe destinar un monto para garantizar medidas que permitan la no interrupción de servicio y que garanticen el ejercicio de derechos.

- Una revisión del marco jurídico interno sobre formas de contratación y cooperación en caso de un ataque.

- Se debe crear un directorio de soporte con proveedores y personas responsables de la respuesta a incidentes dentro del Estado.

- La realización de un censo de infraestructura esencial para la entidad y la creación de una ruta para el reporte y la atención de vulnerabilidades.

2. Las auditorías son indispensables para reducir riesgos

Las auditorías de seguridad digital son fundamentales para identificar qué tan preparada está una organización en términos de personal, procesos y equipamiento al momento de afrontar un incidente. Estas auditorías deberían arrojar una evaluación del nivel de riesgo de la organización. Dicho resultado deberá ser considerado durante el diseño de la política interna de ciberseguridad y del plan de respuesta a incidentes.
Las auditorías deben incluir en todos los casos pruebas de penetración, hacking ético y aseguramiento de la infraestructura. También debe evaluarse la capacidad técnica y de respuesta del personal encargado de manejar incidentes dentro de la entidad.
Las auditorías deben ser llevadas a cabo por personal calificado técnicamente e independiente de la dirección de la entidad. Por supuesto, la consideración e implementación de los hallazgos de la auditoría deben estar a cargo de la entidad y de su dirección.

3. Se necesita un equipo de respuesta a incidentes

Un incidente de ciberseguridad siempre será mejor manejado por personas expertas que conozcan y estén preparadas para reaccionar ante una eventualidad de este tipo. Este equipo debe tener roles claros y un liderazgo competente. Las partes interesadas en un eventual incidente, en especial las directivas dentro de las entidades, deben entender claramente las responsabilidades del equipo de ciberseguridad y estar dispuestas a cooperar en caso de ser necesario.

Para la atención efectiva de un incidente de seguridad es primordial la coordinación entre las oficinas de tecnología (área encargada del funcionamiento adecuado de los sistemas y equipos con que opera la entidad), la de seguridad digital (responsable de ejecutar el plan de seguridad digital y de responder a los incidentes) y las directivas. En caso de ataque, un canal de comunicación seguro y rápido es indispensable entre los tres actores.

Otra clave para una atención adecuada, es el trabajo coordinado entre entidades del sector para evitar la expansión y las ramificaciones del incidente. El relacionamiento para la respuesta al ataque debe darse por medio de los equipos de respuesta a incidentes.

Finalmente, los equipos de respuesta deben establecer un procedimiento para la conservación de las capacidades de respuesta a incidentes. Esto debe incluir evaluación de medidas para mantener y fortalecer los equipos de respuesta, así como la creación de documentos con aprendizajes institucionales y contemplar necesidades de capacitación continua.

4. El plan de respuesta a incidentes debe estar documentado

Debe existir un plan claro y detallado en caso de un incidente. Este plan debe cubrir los roles y responsabilidades de cada actor dentro de la entidad bajo ataque, las directrices sobre la investigación del incidente, el triaje (clasificación del incidente según su gravedad) y planes de mitigación, los planes de recuperación y las claves para la documentación y registro de todo el proceso.
Los protocolos de atención a incidentes deben estar diseñados de acuerdo con las políticas de la entidad encargada de la política de seguridad a nivel nacional.

5. Identificar indicadores de riesgo a la seguridad digital

Es importante identificar señales, datos o sucesos que desatan la reacción a un incidente. Por ejemplo, la pérdida de información, reportes de fuga de información o una falla general en los sistemas de comunicación de la organización.

Sin importar si se trata de un ciberataque general o enfocado en un solo servicio o sistema, siempre se debe hacer una revisión completa, inclusive de aquellos sistemas que parecen no estar afectados por el incidente. El análisis debe determinar los niveles de afectación, riesgo y operabilidad de todos los sistemas, servidores y aplicaciones, de forma tal que se obtenga un inventario total de la infraestructura.

6. Investigación del incidente

Es recomendable buscar información interna y externa respecto del incidente. Esto ayudará a obtener una mejor comprensión del mismo, por ejemplo, si existen otros afectados, cuál debe ser la mejor forma de documentar los hallazgos o si existen experiencias exitosas de respuesta.

7. Triaje y mitigación

La investigación facilitará la clasificación del incidente y consecutivamente marcará las pautas para su mitigación. Por ejemplo, identificar prioridades y asignar responsabilidades puntuales.

Entre las medidas claves para una mitigación exitosa destacamos:

- Informar de forma inmediata a los proveedores de servicios (nube, bases de datos, antivirus, etc) de la entidad sobre el ataque.
- Se debe informar de forma segura y suficiente sobre el incidente a la ciudadanía y los medios. Una comunicación transparente permite evitar la desinformación, el pánico y la especulación.
- Dentro de las posibilidades se debe colaborar con la Fiscalía en la recolección de evidencia física, aislar equipos y tomar pruebas forenses, estas medidas son fundamentales para la investigación del incidente y eventualmente la judicialización de las personas responsables.
- Se deben evaluar y aplicar las recomendaciones del COLCERT para la clasificación de incidentes (triaje) y, en los casos graves o muy graves, se debe notificar a las autoridades respectivas.

Durante el triaje y la mitigación es imperativo tener en cuenta las afectaciones que causa un ciberataque para el normal funcionamiento de la entidad pero también hacia la ciudadanía. La fuga de datos personales, los retrasos en la prestación de servicios o sobrecostos para acceder a servicios básicos. Por tanto, las personas responsables de la respuesta deben asegurarse de tomar las medidas suficientes para mitigar el daño y reducir las afectaciones.

8. Recuperación

Una vez mitigado el incidente se deben recuperar la totalidad de los servicios y la infraestructura que haya sido afectada durante el incidente. La recuperación implica que se pasa de un estado de reacción al de monitoreo normal de los sistemas. Los procedimientos de recuperación están supeditados a las necesidades y contextos de cada organización.

Tras la ocurrencia de un incidente de ciberseguridad es fundamental intentar encontrar la causa, vulnerabilidad o el origen del mismo (sistemas desactualizados, robo de credenciales, etc). Subir o restablecer un sistema sin identificar las fallas o vulnerabilidades lo expone a que se repita el mismo tipo de ataque.

En la priorización de la recuperación de los sistemas deben primar los servicios de nivel nacional, la infraestructura crítica, los vinculados con la prestación de servicios a la ciudadanía y los necesarios para evitar otros posibles ataques o ramificaciones. No debe olvidarse que un ciberataque no solo afecta a la entidad, sino a la ciudadanía que recibe sus servicios o que requiere ejercer sus derechos. Por tanto, en el proceso de responder al ciberataque y recuperar los sistemas siempre se debe intentar durante la contingencia minimizar los daños colaterales para los ciudadanos.

Concluídas las tareas de respuesta, la entidad que recibió el ataque debe evaluar medidas que permitan reducir la carga de estrés y trabajo producto de la intensa situación por la que acaban de pasar.

9. Documentación y reportes

El proceso de documentación de un incidente de ciberseguridad ocurre en todos los estados de incidente, desde antes de que ocurra hasta su recuperación e incluso toda la información *post mortem* que se pueda recopilar.

Los reportes de la documentación de un incidente son la base de futuras investigaciones y la retroalimentación al plan de respuesta a incidentes de una organización. El análisis de la documentación permite extraer información sobre los tipos de incidentes, frecuencia, alcances y atacantes. Esta información es importante a la hora de diseñar políticas públicas y su publicación ayuda a construir una cultura de seguridad digital y respuesta a incidentes.

10. Evaluación del proceso

¿Fue suficiente el equipo usado en la respuesta al incidente? ¿Se identificaron nuevos riesgos en la organización? ¿Se deberían automatizar algunas partes de la respuesta a incidentes? Estas y otras preguntas pueden ser respondidas evaluando el proceso y la documentación hecha en el incidente.

11. Práctica

Como cualquier habilidad, la de responder a incidentes de seguridad digital, requiere de práctica, no basta solo con hacer planes y documentar, la preparación, tanto del equipo de respuesta como de todas las partes interesadas en un incidente son fundamentales en el éxito de una respuesta a un incidente. Se deben simular y practicar los escenarios que se puedan presentar, especialmente los que la evaluación de riesgos de la organización tipifique como críticos.

De igual forma, contar con una ruta de reporte de vulnerabilidades es indispensable para prevenir y preparar a la entidad respecto futuros ataques. Una ruta de vulnerabilidades ayuda a encontrar problemas no resueltos en los sistemas y a arreglarlos antes de que sean usados por un atacante.

CONSIDERACIONES
PARA EL DISEÑO DE UN PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

20 años Fundación Karisma

KARISMA.ORG.CO

karismacol @Karisma

karismacol fundacionkarismaa