Plantilla de plan de respuesta a incidentes de ciberseguridad y seguridad de datos

Esta plantilla de plan de respuesta a incidentes se ha obtenido a partir de la información de dominio público de las políticas de muestra de ciberseguridad del SANS Institute y otras fuentes públicas. Está disponible para su uso, alteración y reformateo de acuerdo con las necesidades específicas de su organización.

Objetivos de la respuesta a ciberincidentes

Cuando se produce un incidente de ciberseguridad, la adopción de medidas oportunas y exhaustivas para gestionar el impacto incidente es fundamental para un proceso de respuesta eficaz. La respuesta debe limitar el potencial de daño asegurando que las acciones sean bien conocidas y coordinadas. En concreto, los objetivos de la respuesta son

1. Preservar y proteger la confidencialidad de la información de los electores y empleados y garantizar la integridad y disponibilidad de los sistemas, redes y datos relacionados de < NOMBRE DE LA EMPRESA>.

2. Ayudar al personal de < NOMBRE DE LA EMPRESA> a recuperar sus procesos de negocio tras un incidente de seguridad informática o de red u otro tipo de violación de datos.

3. Proporcionar una estrategia de respuesta coherente a las amenazas del sistema y de la red que ponen en riesgo los datos y sistemas de < NOMBRE DE LA EMPRESA>.

4. Desarrollar y activar un plan de comunicaciones que incluya la notificación inicial del incidente, así como comunicaciones continuas, según sea necesario.

5. Abordar las cuestiones jurídicas relacionadas con la cibernética.

6. Coordinar los esfuerzos con los equipos externos de respuesta a incidentes informáticos y las fuerzas de seguridad.

7. Minimizar el riesgo reputacional de < NOMBRE DE LA EMPRESA>.

Objeto y ámbito de aplicación

Esta publicación ofrece directrices prácticas para responder a incidentes de ciberseguridad y violación de datos de forma coherente y eficaz. El plan establece un equipo de primeros intervinientes ante un incidente con funciones, responsabilidades y medios de comunicación definidos.

Aunque este plan está orientado principalmente a incidentes y violaciones relacionados con la cibernética, también puede utilizarse para violaciones de datos que no estén relacionadas con sistemas informáticos.

Equipo de Respuesta a Incidentes (IRT)

Un equipo compuesto por personal de la empresa, asesores y proveedores de servicios será responsable de coordinar las respuestas a incidentes y se conocerá como Equipo de Respuesta a Incidentes (IRT). El IRT estará formado por las personas enumeradas en el Apéndice A, con las funciones y responsabilidades indicadas. Este equipo tendrá primarios y secundarios. Los miembros primarios del IRT actuarán como primeros respondedores o miembros informados ante un incidente que justifique la participación del IRT, según la gravedad del incidente. Todo el IRT será informado e involucrado en los incidentes más graves.

Los miembros del IRT pueden asumir funciones adicionales durante un incidente, según sea necesario. La información de contacto, incluida una dirección de correo electrónico principal y otra secundaria, además de los números de teléfono de la oficina y del móvil, se mantendrá y distribuirá al equipo. El IRT recurrirá a personal adicional, consultores u otros recursos, (a menudo denominados Expertos en la Materia - SME) según sea necesario, para los procesos de análisis, remediación y recuperación de un . La función de Tecnología de la Información (TI) desempeña un papel

papel significativo en los detalles técnicos que pueden intervenir en la detección y respuesta a un incidente y puede considerarse una PYME en ese sentido.

Habrá un miembro del IRT designado como Gestor de Respuesta a Incidentes (IRM), que asumirá las funciones de organización y coordinación del IRT durante un incidente en el que se active el IRT para responder al incidente.

Proceso del ciclo de vida de la respuesta a incidentes

La gestión de la respuesta a incidentes cibernéticos es un proceso continuo con un patrón cíclico. Los elementos específicos del proceso de respuesta a incidentes que componen el Plan de Respuesta a Incidentes Cibernéticos incluyen:

1. **Preparación:** El proceso continuo de mantenimiento y mejora de las capacidades de respuesta a incidentes y de prevención de incidentes garantizando que los sistemas, redes, aplicaciones y procesos de tratamiento de datos sean suficientemente seguros y que se imparta formación de concienciación a los empleados. Periódicamente se llevan a cabo ejercicios de práctica (también conocidos como ejercicios de mesa) para el IRT, en los que se presentan varios escenarios de incidentes al Equipo en una sesión de práctica.

2. **Identificación:** El proceso de confirmar, caracterizar, clasificar, categorizar, delimitar y priorizar los incidentes sospechosos.

3. **Notificación:** Alertar a los miembros del IRT de la ocurrencia de un incidente y comunicarse durante todo el incidente.

4. **Contención:** Minimizar las pérdidas financieras y/o de reputación, el robo de información o la interrupción del servicio. Comunicación inicial con los electores y los medios de comunicación, según sea necesario.

5. **Erradicación:** Eliminación de la amenaza.

6. **Recuperación:** Restablecer los servicios informáticos a un estado normal de funcionamiento y la reanudación de las actividades empresariales de forma rápida y segura. Proporcionar medidas de reparación de la reputación y actualizaciones en los medios de comunicación, en caso necesario. Proporcionar servicios de control de crédito a los electores afectados, u otras medidas de reparación, según proceda.

7. **Actividades posteriores al incidente:** Evaluación de la eficacia general de la respuesta e identificación de oportunidades de mejora a través de las "lecciones aprendidas" o la mitigación de los puntos débiles explotados. Incorporación de las enseñanzas extraídas del incidente a los esfuerzos de ciberfortalecimiento y al plan de respuesta, según proceda.

Estos elementos del proceso se representan en la Figura 1, que muestra la naturaleza de bucle cerrado del proceso, en el sentido de que lo aprendido de cualquier incidente anterior se utiliza para mejorar el proceso de prevención y respuesta de posibles incidentes futuros.

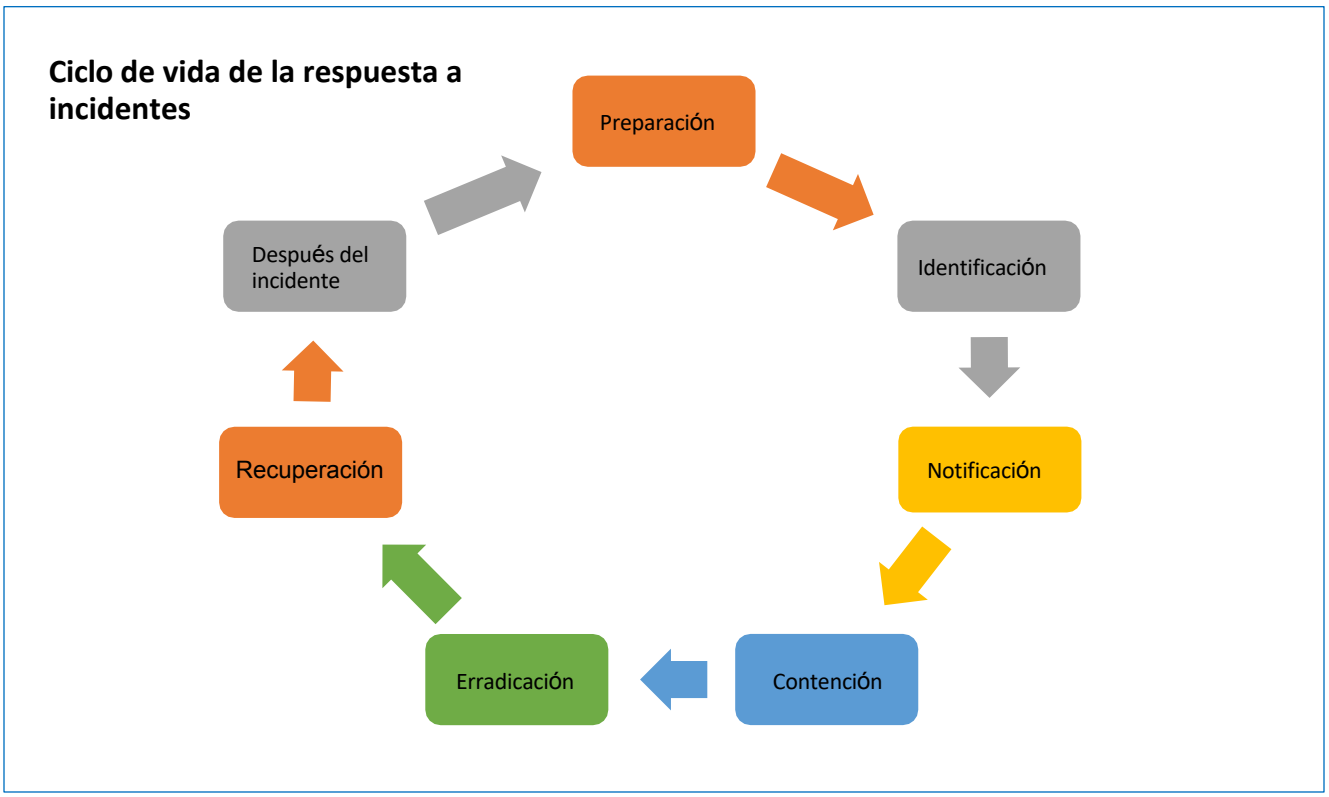

Figura 1

Incidentes y sensibilización

La forma en que se tenga conocimiento de un incidente repercutirá en el proceso de respuesta y en su urgencia. Los ejemplos por los que < NOMBRE DE LA EMPRESA> tiene conocimiento de un incidente incluyen, entre otroslos siguientes:

1. < NOMBRE DE LA EMPRESA> descubre a través de su monitorización interna que se ha producido un incidente cibernético o una violación de datos.
2. <NOMBRE EMPRESA> es notificado por uno de sus proveedores tecnológicos de un incidente o tiene conocimiento del mismo.
3. <NOMBRE DE LA EMPRESA> tiene conocimiento de una violación a través de un constituyente o de un tercero informante.
4. <NOMBRE DE LA EMPRESA> y el público son informados del incidente a través de los medios de comunicación.

Detalle del proceso de respuesta a incidentes

El proceso de respuesta, a nivel de detalle, para un incidente incluye 5 de las 6 fases del ciclo de vida, ya que excluye la fase de Preparación. A continuación se describen los pasos detallados y el calendario general de la respuesta a un incidente. La función de TI se menciona específicamente como parte implicada, separada de otras PYME.

Fase de proceso y Calendario aproximado	Pasos detallados del proceso	Partes implicadas
Identificación (Horas)	1. Identificar y confirmar que el incidente sospechado o denunciado se ha producido y si actividad maliciosa sigue en curso. 2. Determine el tipo, el impacto y la gravedad del incidente consultando **los apéndices B, C y D**. 3. Adoptar medidas de contención básicas y prudentes.	TI y cualquier proveedor de servicios de supervisión
Notificación (Horas - 1 Día)	4. Informar o activar el IRT, según la gravedad del incidente, como se indica en el Apéndice D, y proporcionar el tipo, el impacto y los detalles del incidente en la medida en que se conozcan. 5. Determinar la necesidad de expertos en la materia (SME) que participen en los procesos de contención, erradicación y recuperación.	TI Y TRI
Contención (Horas-2 días)	6. Tomar medidas inmediatas para reducir cualquier actividad maliciosa en curso o evitar la repetición de actividades maliciosas anteriores. 7. Redirigir los sitios web de cara al público, en caso necesario. Proporcionar respuestas iniciales de relaciones públicas y jurídicas según sea necesario.	IRT, TI, PYME
Erradicación (Días -Semanas)	8. Proporcionar una resolución técnica completa de las amenazas y actividades maliciosas relacionadas. 9. Abordar las relaciones públicas, la notificación y las cuestiones jurídicas.	TI, IRT, PYME
Recuperación (Semanas -Meses)	10. Recupere cualquier interrupción de los procesos empresariales y recupere la normalidad de las operaciones. 11. Abordar los problemas jurídicos o de relaciones públicas a más largo plazo, si es necesario, y aplicar las soluciones constitutivas.	PYME, IRT
Después del incidente (Meses)	12. Formalizar la documentación del incidente y resumir lo aprendido. 13. Aplicar lo aprendido a la preparación futura.	IRT

Métodos de comunicación

Los recursos de comunicación de la empresa (correo electrónico, sistema telefónico, etc.) pueden verse comprometidos durante un incidente grave. Se establecerán métodos primarios y alternativos de

comunicación utilizando infraestructura externa y se anotarán en la lista de contactos de los miembros del IRT para proporcionar métodos específicos decomunicación durante un incidente. Se indicará al IRT y a cualquier otra persona implicada en la resolución de un incidente qué método de comunicación se utilizará durante el incidente.

Registro de información

El registro de información es muy importante durante un incidente, no sólo para los esfuerzos efectivos de contención y erradicación, sino también para las lecciones aprendidas después del incidente, así como para cualquier acción legal que pueda surgir contra los perpetradores. Cada miembro del IRT será responsable de registrar información y referencias cronológicas sobre sus acciones y hallazgos durante un incidente, utilizando el Formulario de Registro de Incidentes del IRT en el Apéndice E.

Ejercicios de respuesta a incidentes

El IRT debe realizar ejercicios "de mesa" para practicar el proceso de respuesta de manera periódica, pero al menos anualmente, para que todos los miembros del IRT se familiaricen con las actividades que ocurrirían durante un incidente real y sus responsabilidades relacionadas. Los ejercicios pueden brindar la oportunidad de mejorar la coordinación y comunicación entre los miembros del equipo.

Resumen

No se puede escribir un guión perfecto para la actividad detallada que se encuentra y las decisiones que habrá que tomar durante un incidente, ya que cada incidente tendrá su propia singularidad. Este plan servirá de marco para la gestión de incidentes de ciberseguridad y violación de datos, permitiendo que los detalles de confirmación, contención, erradicación y comunicación se adapten a cada situación específica.

Apéndice A - < NOMBRE DE LA EMPRESA> Equipo de Respuesta a Incidentes Cibernéticos (IRT)

Miembros del equipo y funciones - *Sustituya los nombres y títulos del personal a continuación según corresponda. Es posible que no todos los puestos estén disponibles en su organización y/o que la misma persona desempeñe varias funciones dentro del IRT.*

Miembros principales del equipo

1. <Jefe de Informática>
    a. Mantener políticas y procedimientos proactivos de ciberseguridad
    b. Descubrir y/o verificar incidentes cibernéticos
    c. Notificar los incidentes a los miembros del IRT y proporcionar información actualizada
    d. Coordinar las actividades de reparación informática forense y técnica.
    e. Aplicar medidas correctoras a la infraestructura tecnológica

2. <Gestor de Respuesta a Incidentes> (IRM)
    a. Coordinar las comunicaciones y actividades del IRT cuando se active

3. <Directivo de nivel ejecutivo encargado de la gestión financiera>
    a. Impacto financiero y exposición de datos financieros

4. <Directivo de nivel ejecutivo encargado de la comunicación externa y las relaciones públicas>
    a. Relaciones públicas
    b. Gestión de los medios de comunicación
    c. Comunicación externa e interna

5. <Gerente de nivel ejecutivo encargado de recursos humanos>
    a. Comunicación a los empleados
    b. Problemas de exposición de los datos de los empleados

6. <Directivo de nivel ejecutivo a cargo de las operaciones de la empresa>
    a. Evaluación del impacto operativo y/o de la exposición global a los datos

7. <Gerente de nivel ejecutivo a cargo de la seguridad física>
    a. Acceso y control de edificios

Miembros del equipo secundario

8. <Proveedor de monitorización de eventos de seguridad y/o proveedor de informática forense>
    a. Detección
    b. Mitigación
    c. Técnica forense

9. <Representante legal>
    a. Asesor jurídico
    b. Asuntos contractuales

10. <Vendedor de relaciones públicas>
    a. Asesor de relaciones públicas

11. <Proveedor de ciberseguros>
    a. Asesor de ciberseguro

La información de contacto y los métodos de comunicación de los miembros de la IRT deben distribuirse al equipo por separado como información confidencial.

Apéndice B - Categorización de incidentes

CATEGORÍAS COMUNES DE INCIDENTES CIBERNÉTICOS

Tipo de incidente	Tipo Descripción
Acceso no autorizado	Cuando una persona o entidad obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso de la empresa.
Denegación de servicio (DoS, DDoS)	Ataque que impide o deteriora con éxito la funcionalidad normal autorizada de redes, sistemas o aplicaciones agotando los recursos.
Código malicioso	Instalación satisfactoria de software malicioso (por ejemplo, un virus, un gusano, un troyano u otra entidad maliciosa basada en código) que infecta un sistema operativo o una aplicación.
Uso indebido o inadecuado	Cuando una persona infringe las políticas informáticas aceptables, incluido el acceso no autorizado o el robo de datos.
Sospecha de violación de la IIP	Un incidente en el que se sospecha que se ha accedido a Información de Identificación Personal IIP).
Sospecha de pérdida de información sensible	Incidente que implica una presunta pérdida de información sensible (no IIP) que se ha producido debido a un acceso no autorizado, un código malicioso o un uso inadecuado (o inapropiado), cuando se desconoce la causa o el alcance.

Apéndice C - Definiciones del impacto del incidente

Objetivo de seguridad	Descripción general	Ejemplos de impacto potencial		
		Bajo	Medio	Alta
Confidencialidad: *Preservar las restricciones de acceso y divulgación de la información, incluidos los medios para proteger la intimidad personal y la propiedad. información.*	La divulgación no autorizada de información podría tener el siguiente efecto adverso sobre las operaciones de la organización, los activos de la organización o los individuos.	Limitado a uno o varios usuarios u ordenadores forma aislada, con fácil reparación.	Involucrar o afectar a un grupo de usuarios, dando lugar al acceso a información privilegiada. Exposición externa limitada o nula.	Una violación grave de información privilegiada con exposición externa.
Integridad: *Protección contra la modificación o destrucción indebidas de la información; incluye garantizar el no repudio y la autenticidad de la información.*	La modificación o destrucción no autorizada de información podría tener el siguiente efecto adverso sobre las operaciones de la organización, los activos de la organización o los individuos.	Alteración o borrado involuntario o no malintencionado o de datos de la empresa fácilmente subsanable.	Un acto (o serie de actos) continuado de alteración indebida de datos de naturaleza maliciosa o negligente que tendrá un impacto empresarial moderado.	Una alteración o destrucción masiva de datos de la empresa de carácter malicioso u obstruccionista.
Disponibilidad: *Garantizar el acceso oportuno y fiable a los sistemas de información y su utilización.*	La interrupción del acceso o del uso de la información o de un sistema de información podría tener el siguiente efecto adverso en las operaciones de la organización, los activos de la organización, o particulares.	Interrupción aislada o inaccesibilidad que afecta a un número limitado de usuarios durante un breve periodo de tiempo. (< 2 horas)	Una interrupción o inaccesibilidad generalizada de un sistema empresarial principal que dure más de 2 horas, pero menos de un día.	Interrupción grave o inaccesibilidad de los sistemas de negocio de la empresa durante un día o más.

Apéndice D - Matriz de clasificación de gravedad y respuesta a incidentes IRT

Nivel de gravedad (5=más grave)	Características típicas de los incidentes	Ejemplo de impacto	Respuesta a incidentes	¿Activar IRT?
5	Ataques DDoS contra servidores locales o alojados. Ataques activos contra la red infraestructuras. Acceso a datos internos de la empresa por parte de terceros malintencionados.	Ataque a nivel de toda la empresa que afecta a varios departamentos e impide el acceso a los sistemas e interrumpe las operaciones comerciales. El acceso o robo de datos de propiedad.	Respuesta directa de la IRT y el IRM. Remediación coordinada por IT, Forensics y SME. Posible asesor jurídico, Participación de las fuerzas del orden	Equipo completo activo
4	Afecta a datos o servicios de un grupo de personas y amenaza a datos sensibles, o implica a cuentas con privilegios elevados con amenaza potencial para los datos sensibles	Aplicación empresarial comprometida. Acceso indebido o no autorizado a los datos.	Respuesta coordinada por IRM, IT y PYME; IRT aconsejado. Notificación específica a la Asesoría Jurídica en caso de violación de la IIP.	Todo el equipo informado y asesorado
3	Afecta a los datos o servicios de una sola persona, pero implica cantidades significativas de datos sensibles, puede incluir PII.	Ordenador o cuenta de empleado con acceso a datos sensibles comprometidos, robo físico del dispositivo, soportes desprotegidos o datos en papel.	Respuesta coordinada por IT o IRM, con información enviada a los miembros del IRT. Notificación a la Asesoría Jurídica en caso de violación de la IIP	Equipo primario informado
2	Afecta a datos o servicios de un grupo de personas sin datos sensibles implicados.	Compromiso de una cuenta o dispositivo con acceso a carpetas compartidas.	Respuesta coordinada por IT. IRM avisado e IRT informado. Proceso de documentación de TI utilizado para registrar resultados.	Equipo primario informado
1	Afecta a los datos o servicios de una sola persona sin datos sensibles más allá de ellos; la atención se centra en corrección y futuro prevención	Ordenador comprometido sin datos sensibles, etc.	Documentación del problema y conclusiones. Respuesta/remediación coordinada por IT, IRM informados del incidente.	No
0	Incidentes de foco, origen y/o efecto muy leve o indeterminado para los que no existe un seguimiento práctico.	Ordenador dañado que requiere la revisión de los registros de acceso al sistema, análisis antivirus u otras reparaciones.	Documentación a través de los procesos normales de soporte informático para registrar las acciones y su resolución. Restablecimiento de contraseñas según sea necesario.	No

Apéndice E - Formulario de registro de incidentes IRT

Incidente: _____

Fecha de descubrimiento: _____

Grabado por: _____ Página _____de _____ Páginas

Información y eventos registrados

Fecha/Hora	Detalle

Historial de versiones del documento

Versión	Fecha	Cambios/Anotaciones
1.0	<Fecha de publicación>	Lanzamiento inicial