Plan de Respuesta a Incidentes

<NOMBRE DE LA EMPRESA>

Introducción

Este plan de respuesta a incidentes presenta las actividades y procedimientos para responder y gestionar un incidente de seguridad de la información dentro de *<NOMBRE EMPRESA>*.

El objetivo del plan es proveer los elementos que permitan la identificación, valoración, respuesta y tratamiento oportuno minimizando los impactos negativos a la organización y dar a los responsables de la respuesta y el tratamiento de los incidentes a nivel técnico y de gestión los puntos clave que permitan lograr la respuesta en estas condiciones.

Infraestructura cubierta por el plan

<En esta sección se provee una descripción general sobre la infraestructura que es cubierta con el plan de respuesta a incidentes, considerando aquellos sistemas críticos - infraestructura, plataforma, aplicaciones - de forma tal que si es necesario realizar la revisión de un diagrama de infraestructura, red, la arquitectura sobre un sistema su acceso sea rápido.

Dado que puede ser usual contar con esta información en otra documentación, se pueden incluir los links a dicha documentación para asegurar el uso de las últimas versiones>

Diagramas de infraestructura y arquitectura

<Link a los diagramas que permitan visualizar sistemas, red, flujos de datos y esquemas de almacenamiento.

Si se cuenta con servicios tercerizados en esquemas como SaaS y estos tienen integraciones con infraestructura propia, como se dan esas conexiones>

Esquemas de autenticación y autorización

<Incluir la información base y las referencias si se encuentra en documentación externa sobre los mecanismos de autenticación y autorización utilizados en la organización para detectar puntos de gestión. Por ejemplo, si se cuenta con esquemas de gestión de identidades, aplicaciones que realicen autenticación local, entre otros>

Esquemas de registro y monitoreo

<Incluir la información base y las referencias si se encuentra en documentación externa sobre las fuentes de registro que se usan, donde se almacenan y las herramientas o sistemas que se están utilizando para el monitoreo>

Inventario de activos tecnológicos

<Link al inventario de dispositivos con los que cuenta la organización, tanto a nivel de infraestructura como equipos de cómputo.

Es importante considerar que estos cuenten con al menos la siguiente información: nombre activo, IP, segmento de red donde se ubica, sistemas operativos asociados, versiones, localización, y responsables>

Roles y responsabilidades

<En esta sección indique los roles y responsabilidades que deben estar a cargo de la respuesta a incidentes. Esto considera en primera instancia, quienes están llamados a declarar y hacer la valoración del incidente, y a partir de eso los encargados de atender el incidente en cada una de las etapas posteriores (contención, erradicación, recuperación y fase post incidente)>

El incident handler es el líder del equipo de respuesta con el conocimiento técnico y de seguridad sobre la infraestructura y los sistemas y con conocimientos sobre el manejo global del plan de respuesta a incidentes.

Los analistas de primer / segundo nivel son el equipo de apoyo al incident handler que en primera instancia pueden recibir notificaciones sobre un incidente y realizar la valoración (triage) de este para establecer su nivel de criticidad acorde con los parámetros definidos en la organización para a partir de esto realizar su escalamiento.

<Dependiendo del tamaño de la empresa pueden existir analistas sólo de primer nivel que trabajan directamente con el incident handler, o contar con los dos niveles de analistas con niveles de especialización en la respuesta.

Organizaciones que cuentan con un Security Operation Center (SOC) usualmente cuentan con niveles de especialización, donde el primer nivel se encarga de monitoreo continuo y el segundo soporta la atención de incidentes cuando este es declarado>

El gestor de servicio es el rol o cargo que cuenta con el conocimiento sobre el servicio afectado, las aplicaciones o sistemas que lo soportan y el impacto que puede traer al negocio la pérdida de disponibilidad, confidencialidad o integridad. Por esto cuenta con la autoridad para tomar decisiones sobre cursos de acción en la atención del incidente, tales como aislar el servicio.
El equipo de comunicaciones se encarga de apoyar la respuesta oportuna a los diferentes públicos objetivo (internos y externos) con la generación y publicación de información sobre el incidente y su gestión a través de los canales de comunicación definidos en la empresa.

<Como canales de comunicación se puede considerar el portal web, las redes sociales y declaraciones de prensa ante públicos externos, comunicados formales por correo electrónico, entre otros. Ante públicos internos los canales de comunicación interna definidos como herramientas corporativas, sesiones sincrónicas extraordinarias, entre otros.

Cuando se plantea respuesta oportuna se refiere a que es recomendado una vez se presente un incidente, adelantarse a los atacantes en la divulgación de la brecha, y que la empresa sea

quien de los primeros pasos en la declaración sobre el incidente, así como actualizaciones periódicas de las acciones que realiza la organización frente a su gestión guardando cuidado de que se informa y el lenguaje utilizado>

Contactos

El equipo de respuesta a incidentes incluye los siguientes contactos:

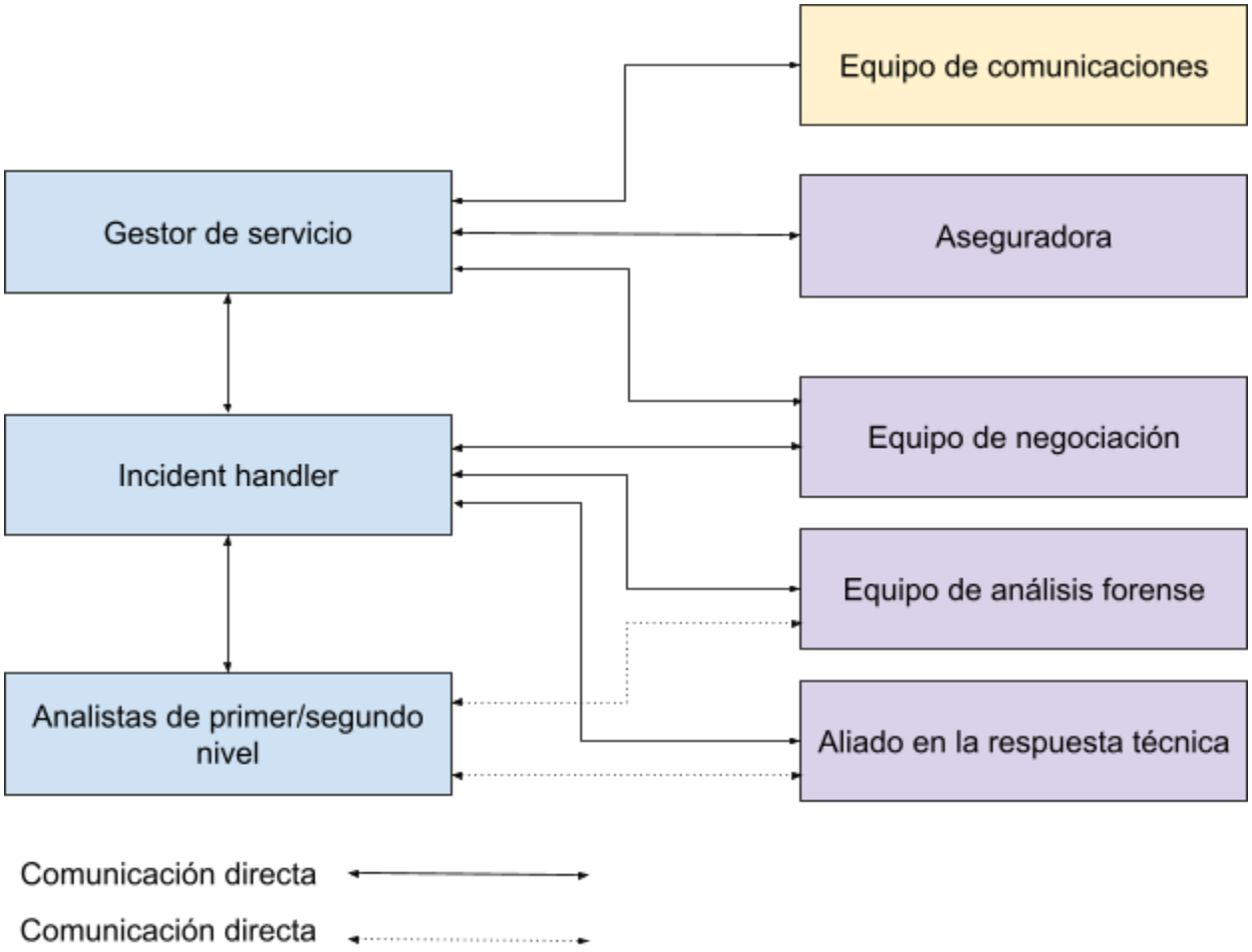
Incident handler:	
Email:	
Tel:	

Analista primer/segundo nivel:	
Email:	
Tel:	

Gestor de servicio:	
Servicio/sistema:	
Email:	
Tel:	

Comunicaciones:		
Ambito:	Interno	Externo
Email:		
Tel:		

Árbol de llamadas y escalamiento



Contactos de aliados para la respuesta

Dependiendo de la naturaleza del incidente, los siguientes son los contactos aliados para la respuesta:

Nombre aseguradora:	
Contacto asesor:	
Email:	
Tel:	

Equipo negociación:	

Contacto asesor:	
Email:	
Tel:	

Equipo Análisis forense:	
Contacto:	
Email:	
Tel:	

Aliado en respuesta técnica:	*<Por ejemplo, si la organización cuenta con servicios en cloud, el servicio de soporte del proveedor de cloud se convierte en un aliado en la respuesta técnica. Aquí se puede incluir la información sobre los canales de comunicación para contacto rápido>*
Contacto:	
Email:	
Tel:	

<Las consideraciones sobre estos contactos corresponden a lo siguiente:

- *Si la organización tiene contratado un ciberseguro, contar con los datos del asesor que puede brindar apoyo inmediato resulta relevante.*
- *Cuando se trata de un incidente tipo ransomware en el cuál los atacantes buscan extorsionar a la organización, es importante contar con un equipo o encargado de negociación (interno o externo) que asesore las comunicaciones con los atacantes y sirva como vocero en el proceso.*
- *Algunos incidentes pueden demandar la necesidad de un análisis forense digital. El responsable de forense puede ser interno o externo y se considera como parte de los contactos aliados por el nivel de especialización del rol. Usualmente solo a nivel de grandes organizaciones se cuenta con este rol interno. En organizaciones de mediano y pequeño tamaño, es contratado con un tercero cuando es requerido. Sin embargo, es importante así no se cuente con un contrato vigente, contar con un proveedor que rápidamente pueda apoyar en una situación, evitando la posibilidad de salir al mercado a realizar una búsqueda desde cero en un momento de emergencia*

- *Los aliados en respuesta técnica pueden tratarse de proveedores, terceros, grupos de apoyo incluida la competencia, que por sus capacidades técnicas en respuesta a incidentes y seguridad puedan entrar a apoyar a la organización en la respuesta y gestión>*

Contactos entes de control

Ante incidentes de seguridad que impliquen brechas de privacidad realizar el reporte a:

Ente de control:	*<Para el caso colombiano, la Superintendencia de Industria y Comercio>*
Contacto:	
Email:	
Tel:	
Información que debe ser reportada:	
Tiempos establecidos de reporte:	

<De acuerdo con el sector al cuál pertenece la organización se requiere reportar los incidentes de seguridad o indisponibilidad de los servicios a los respectivos entes de control. Por ejemplo, en el caso colombiano, para el sector financiero debe ser reportado ante la Superintendencia Financiera a través de los canales establecidos por la entidad.

Los medios de reporte, las características y condiciones, deben ser indicadas aquí para asegurar que se utilizan los canales adecuados y se realiza bajo los tiempos estipulados. Esto es parte de la información que debe estar al alcance del equipo de comunicaciones>

Requerimientos de comunicación

<En esta sección indique todos los requerimientos de comunicación ante un incidente de seguridad partiendo de la premisa que la organización debería ser la primera en hablar sobre el mismo previo a que se filtre la información por terceros.

Considere establecer cuales son los públicos objetivo, los canales y voceros autorizados así como las plantillas de comunicación y/o guiones base que permitan una comunicación rápida en el momento requerido.

Dado que puede ser usual contar con esta información en otra documentación como el plan de comunicación en crisis (si la organización cuenta con este) o el procedimiento y gubias de comunicación del área encargada, se pueden incluir los links a dicha documentación para asegurar el uso de las últimas versiones>

Públicos objetivos de comunicación

Los siguientes son los públicos objetivos para comunicaciones internas y externas, los canales autorizados para su contacto y los voceros autorizados:

<Por cada público objetivo se es recomendado definir un único canal autorizado con el fin de centralizar las comunicaciones. Sin embargo, pueden establecer tantos canales de comunicación como se considere pertinente.

Se recomienda considerar voceros con habilidades y cualidades acordes para realizar las comunicaciones con cada uno de los públicos objetivos. Dentro de los elementos a considerar el manejo de lenguaje técnico o formal, el nivel de reconocimiento del rol o cargo frente al público al cuál se dirige y capacidades oratorias así como de interacción. En todos los casos es recomendado que la preparación de comunicados esté acompañada por especialistas en comunicaciones y relaciones públicas>

Publico Objetivo	**Canal autorizado**	**Vocero autorizado**
Clientes	*<Indicar el canal autorizado para comunicarse con cada público objetivo>*	*<Indicar el rol o cargo autorizado para generar comunicaciones con cada público objetivo>*
Público en general		
Prensa		
Proveedores		
Entes de control		
Junta Directiva - Accionistas		
Empleados		

Plantillas de comunicación

<Link a las plantillas de comunicación predefinida de acuerdo con escenarios de incidentes analizados como posibles en la organización y que puedan resultar de alto impacto a nivel de reputación, marca y relacionamiento.

Se recomienda considerar dentro de las plantillas contar con una base para incidentes tales como brechas de datos por ataques de ransomware o phishing. Además de contar con plantilla por público objetivo>

<Para la creación de comunicados dirigidos a diferentes públicos de interés actualmente se puede utilizar herramientas como chat GPT - chat.openai.com>

Procedimientos de respuesta a incidentes

El proceso de respuesta a incidentes considera los siguientes pasos de alto nivel:

Severidad y priorización por incidentes

<Aquí se detalla cómo se clasifica la severidad de un incidente, a partir de ello como se realiza su priorización y los esquemas para escalamiento definidos en la organización.

La priorización de los incidentes debería considerar el análisis de impactos previo que ha sido realizado. Se recomienda considerar al menos los siguientes tipos de incidentes:

- *Ransomware*
- *Phishing*
- *Brecha de datos*
- *Denegación de servicios>*

Detección, declaración y análisis

Como respuesta inicial identifique si ha ocurrido o está ocurriendo un incidente. Este proceso comienza después de que alguien nota y notifica alguna anomalía o esta es detectada a través de los esquemas de monitoreo.

<Definir los medios a través de los cuales el personal puede notificar cualquier anomalía o incidente en horario laboral y no laboral>

- Determinar si el evento es realmente indicativo de un incidente y, de ser así, el tipo y la gravedad del incidente
- Basado en la severidad del incidente, determinar el nivel de respuesta (quienes deben ser involucrados) incluyendo la toma de decisión sobre si el objetivo es restaurar los

sistemas o se incluirán actividades forenses formales para el manejo adecuado de cadena de custodia.
- Realizar un análisis rápido sobre activos e información comprometidos para determinar un alcance previo
- Iniciar el análisis de los impactos y las consecuencias que se pueden presentar por la naturaleza del incidente
- Declarar o notificar el incidente a través de los canales definidos a los públicos objetivos
- Según el tipo de incidentes identificar los procedimientos a seguir

Contención

A partir del análisis de activos comprometidos:

- Con la determinación previa del alcance del incidente, iniciar labores de contención con actividades de aislamiento de los activos afectados
- A partir de la información sobre infraestructura del negocio analizar las interacción y relaciones de los componentes afectados con otros que deban ser revisados para validar si se encuentran comprometidos y deben ser aislados
- Mantener monitoreo sobre infraestructura para identificar otros activos comprometidos

Erradicación y Recuperación

Considerar:

- La instalación de versiones limpias de sistemas operativos
- La instalación de actualizaciones de seguridad
- La deshabilitación de servicios innecesarios
- Si se toma en consideración el uso de copias de seguridad, validar que estas no han sido comprometidas previo a su uso para la recuperación
- Realizar actualización de credenciales de acceso

Playbooks

<Los playbooks dentro de la gestión de incidentes son aquellos que a partir de un conjunto de actividades y reglas describen el curso de acción a ejecutar ante un incidente, a modo de guía como paso a paso.

Dentro de los playbook se puede considerar las actividades de detección y análisis, contención, erradicación y recuperación como un todo, o pueden considerarse playbooks independientes por fase de acuerdo con el nivel de detalle que se desarrolle en estos y relacionarlos en cada uno de los pasos presentados previamente.

Incluir aquí los links a los playbooks definidos en la organización para la atención de los incidentes que a partir de análisis se consideren relevantes para la organización por su nivel de exposición, el tipo de información que maneja y el análisis de impacto que realicen. Se recomienda considerar playbooks al menos para los siguientes tipos de incidentes:

- *Ransomware*
- *Phishing*
- *Brecha de datos*
- *Denegación de servicios*

El nivel de detalle de los playbooks debe analizarse basado en las necesidades de la organización. En algunos casos puede ser suficiente la mención a una actividad macro, en otros se requiere mayor granularidad. En todos los casos se recomienda probar los playbooks para validar que el curso de acción y el nivel de detalle definido es apropiado. Las pruebas se pueden realizar a través de tabletops o simulaciones>

Enlace con la gestión de cambios

<Link a los procedimientos específicos que tratan sobre cambios de emergencia ante incidentes de seguridad de la información>

Enlace con la continuidad de negocio

<Link a los procedimientos específicos que tratan sobre escenario de contingencia y continuidad y las acciones a considerar ante incidentes de seguridad de la información>

Actividades para análisis post-incidente

Efectividad en la atención del incidente

Las preguntas claves que se consideran para analizar cómo fue atendido el incidente:

- Se conoce en detalle de qué fue lo que sucedió
- Se reconoce la línea de tiempo en la cuál se presentaron los hechos
- El equipo de respuesta actuó de acuerdo con lo planeado
- Se siguieron los procesos establecidos según la naturaleza del incidente. Los procedimientos actuales son suficientes
- Se realizó alguna acción o toma de decisión errada que afectara la respuesta, contención o recuperación
- Qué se haría diferente la siguiente vez si el incidente se repitiera

Mejoras a ser analizadas

Las preguntas claves que se consideran como parte del análisis de mejoras consideran:

- Ante compromiso de credenciales, debilidad en estas, uso de credenciales por defecto, accesos sin credenciales, entre otros.
- Configuraciones en sistemas por defecto, fallas en configuración, posibilidad de exportar o modificar configuraciones sin restricciones
- Niveles de protección sobre directorios y archivos
- Actualizaciones de versiones de software
- Protocolos y servicios que son vulnerables actualmente o se identificaron como tal por un incidente
- Actualización de procedimientos y esquemas de respuesta a partir de lo anterior

Gestión de consecuencias

Las preguntas claves que se consideran para analizar cómo fue atendido el incidente y cuál ha sido el manejo de consecuencias considera:

- Se dió y está dando respuesta en tiempos y con información adecuados a los públicos objetivo
- Se cuenta con claridad sobre los acuerdos contractuales con clientes para identificar incumplimientos que den lugar a penalidades o demandas
- Se ha mantenido informados a los entes de control que apliquen de acuerdo con los requerimientos legales

<Es importante considerar que así el incidente se contenga, aspectos a nivel interno y externo requieren monitoreo y seguimiento para procurar que los niveles de efectividad en la atención sean visibles ante el público según se requiera>