PROTOCOLO DE ACTUACIÓN FRENTE A INCIDENTE EN PROVEEDOR

Una iniciativa de:

isms forum

PROTOCOLO DE ACTUACIÓN FRENTE A INCIDENTE EN PROVEEDOR.

Con la participación de los siguientes profesionales y organizaciones:

Dirección y coordinación:

Francisco Lázaro
Ángel Pérez

Colaboradores:

Edwin Blom
Rafael Hernández
Manuel Fernández
David Esteban

Revisoras:

Elena Matilla
Fanny Y. Pérez

Editor:

Daniel García Sánchez, Director General de ISMS Forum

Diseño y maquetación:

Raquel García Robles, Asistente de comunicación de ISMS Forum

isms forum

ÍNDICE

I. INTRODUCCIÓN

El presente documento responde a la necesidad de hacer frente al problema de la gestión de un incidente de seguridad que esté afectando a un proveedor de tu organización. Esta prestación se realiza con acceso a sus instalaciones, a sus redes o sistemas.

Cuando el incidente en este proveedor es grave, la gestión del mismo por parte del proveedor involucra a la Entidad que debe saber cómo actuar ante esta situación.

El documento ofrece una guía rápida de recomendaciones de coordinación con el proveedor afectado por el incidente, así como de medidas de monitorización, contención y vuelta a la normalidad en la propia Entidad.

Este protocolo debe ser adaptado a las peculiaridades de la infraestructura y organización de cada Entidad e integrada en el Plan de Respuesta a Incidentes específico de la misma; es por ello, que sus contenidos deben ser tomados como un ejemplo.

Nuestra Entidad podría verse amenazada por alguno de estos incidentes acontecido en la infraestructura del proveedor:

- Malware.
- Deficiencias en el proveedor.
- Destrucción de información.
- Fugas de información.
- Vulnerabilidades en los sistemas del proveedor.
- Errores de mantenimiento / actualización del programa (software).
- Suplantación de la identidad del usuario.
- Abuso de privilegios de acceso.
- Acceso no autorizado.
- Ataques de denegación de servicio distribuido (DDoS).
- Divulgación de información.
- Fraude interno.

II. OBJETIVO

El principal objetivo del presente procedimiento es establecer los pasos que debe seguir la Entidad para evitar que el incidente sufrido por el proveedor pueda afectar a las redes y sistemas de información de esta y en consecuencia a los procesos y operaciones de negocio de la misma o al menos reducir sus efectos negativos.

Para ello se recogen las principales acciones que deben llevarse a cabo, sobre el acceso físico a las instalaciones, y sobre el acceso a las redes y sistemas de información de la Entidad, por parte del personal del proveedor afectado por el incidente de seguridad.

III. ALCANCE

El presente procedimiento tiene como alcance al personal de los proveedores que hayan sido afectados por el Incidente de Seguridad, que desarrollan sus actividades en las instalaciones de la Entidad, y los equipos que requieren acceso a la red, sistemas de información e instalaciones de esta.

IV. DESCRIPCIÓN DEL PROCEDIMIENTO

Antes de describir las etapas, fases y tareas, debemos hacer notar que el orden de alguna de las tareas puede ser diferente a la descrita, pues para cada Entidad o incidente las condiciones pueden alterar ese orden; por ejemplo, lo adecuado es conocer el nombre del responsable de seguridad del proveedor ANTES del incidente y sin embargo, en la tabla se muestra lo que ,habitualmente, se da: se conoce después.

ETAPA 1

Identificación y Notificación

FASE	TAREAS	RESPONSABLE
Notificación Incidente (interno al proveedor)	Notificar desde el Departamento de Seguridad del Proveedor el incidente de seguridad en los equipos y sistemas, identificar clase de incidente de seguridad se trata.	Proveedor del Servicio Departamento de seguridad del Proveedor.
	Notificación Incidente desde un CERT de referencia, SOCs, prensa o grupos de seguridad.	Cert de Referencia o Security Operation Center.
Identificación Recursos Afectados	Identificar al Responsable de Seguridad del proveedor y comunicarlo a la Entidad. Él es el punto de contacto del proveedor con la Entidad. Si no pudiera ser el responsable de seguridad deberá ser alguien con "responsabilidad". **Recomendación:** Tenerlo previamente: la Entidad desde que se firma el contrato de prestación de servicios debe conocer los datos de contacto del Responsable de Seguridad del Proveedor y si se producen cambios a lo largo del servicio se debe comunicar.	Proveedor del Servicio Departamento de seguridad del Proveedor.
	Informar al Responsable de Seguridad del proveedor del punto de contacto de seguridad de la Entidad (CISO o equivalente) del incidente. **Recomendación:** Tenerlo previamente: el proveedor desde que se firma el contrato de prestación de servicios debe conocer los datos de contacto del Responsable de Seguridad de la Entidad y si se producen cambios a lo largo del servicio se debe comunicar.	Departamento de seguridad de la Entidad - CERT.
	Elaborar un listado de personal que forma parte de cada uno de los servicios que proporciona el proveedor afectado. **Recomendación:** Tenerlo previamente. Siempre tener listado actualizado.	Personal de la Entidad Responsable del servicio que proporciona el Proveedor.
	Informar a los usuarios del proveedor del contacto del Responsable de Seguridad, para poder ponerse en contacto con él en caso de resultar necesario.	Departamento de seguridad de la Entidad - CERT.
	Verificar el personal del listado contra los usuarios en las herramientas de Gestión de Identidad y Directorio Activo de la Entidad.	Departamento de Tecnología de la Entidad - Operación de GID (Gestión de la Identidad Digital).

Identificar los mecanismos de comunicación que tienen conexión entre la Entidad y el proveedor afectado (túneles IPSEC y VPN).

Investigar cualquier síntoma de alteración en el flujo de comunicación de los Sistemas de Información de la Entidad.

→ Departamento de seguridad de la Entidad – CERT/SOC.

Registro y Reporting

Registrar la información sobre el incidente en la plataforma de gestión de incidentes.

Se entenderá que, aunque los sistemas de información y redes de la Entidad no se hayan visto afectados, dado que se deben iniciar acciones de bloqueo del proveedor, debe identificarse como un incidente. Si bien, en base a las características del incidente acontecido en el proveedor, la entidad debe decidir si se activan las medidas preventivas de bloqueo del proveedor.

→ Departamento de seguridad de la Entidad.

Elaborar informe detallado del incidente. Este informe será contrastado con el aportado por el proveedor.

Si el incidente está teniendo un impacto grave en la Entidad, notificar el incidente al Comité de Seguridad o de Crisis, según se haya establecido en los procedimientos internos de cada Entidad. Se mantendrá informado de los avances, medidas y repercusión del Incidente. Ej: cada 4 horas los primeros 3 días, y cada 8 horas el siguiente. Después se informará 1 vez al día hasta la finalización del incidente.

Evaluar la comunicación al Comité de Crisis.

Revisar las obligaciones regulatorias o normativas existentes según el tipo de incidente para proceder a la notificación en el plazo requerido. En función de la peligrosidad de la amenaza, considerar la notificación proactiva y responsable a stakeholders clave de la Entidad (principales clientes, proveedores, etc.).

→ Departamento de seguridad de la Entidad – CERT/SOC.

ETAPA 2

Análisis y clasificación

Con la información enviada por el proveedor se llevará a cabo una clasificación del mismo para conocer su naturaleza y gravedad. Para ello, se debe realizar lo indicado en el Procedimiento de Gestión ante Incidente.

ETAPA 3

Responder y Contención

FASE	TAREAS	RESPONSABLE
Medidas Tecnológicas	Cortar el tráfico de los túneles IPSEC en ambas direcciones.	Departamento de Tecnología de la Entidad - Operación de comunicaciones. Departamento de Tecnología del Proveedor.
	Bloquear los usuarios en la Gestión de Identidad, directorio activo, o similar con lo que asimismo se consigue bloquear el acceso por VPN.	Departamento de Tecnología de la Entidad - Operación de GID (Gestión de la Identidad Digital).
	Bloquear los indicadores de compromiso (IOC) que se reciban de CERTs de referencia acreditados y del propio proveedor o del SOC. Dependiendo del tipo de IPS se bloquea en: • Firewall. • Proxy. • Antimalware. • IPs. Debería existir un inventario de servicios por proveedor con los elementos de arquitectura que tienen (Inventario de activos y dependencias) para en caso de necesidad bloquearlos rápidamente.	Departamento de Tecnología de la Entidad - Operación de seguridad.
	Bloquear correo entrante de los dominios del proveedor en las MTAs- Mail Transfer Agent (servidores de correos).	Departamento de Tecnología de la Entidad - Operación de Sistemas.
	Dar de baja a los usuarios del proveedor de la NAC de la Entidad.	Departamento de Tecnología de la Entidad - Operación de comunicaciones.
Otras Medidas	Desactivar las tarjetas de acceso a las instalaciones a los usuarios del proveedor del servicio, para impedir el acceso físico a las instalaciones. De esta forma, se revisará quién accede para controlar los dispositivos (portátiles, tablets, etc) y evitar infecciones.	Departamento de Tecnología de la Entidad - Operación de GID (Gestión de la Identidad Digital).

ETAPA 4

Supervisión de las medidas y Monitorización

FASE	TAREAS	RESPONSABLE
Supervisión de las medidas	Verificar que no existe tráfico en los túneles IPSEC en ambas direcciones.	Departamento de Tecnología de la Entidad y Departamento de Tecnología del Proveedor.
	Comprobar que los usuarios permanecen bloqueados en la Gestión de la Identidad, directorio activo, etc.	Departamento de Tecnología de la Entidad.
	Comprobar diariamente las MTAs (servidores de correos) entrantes para verificar el bloqueo de las direcciones de correo.	
	Verificar el bloqueo de los usuarios del proveedor en la NAC de la Entidad.	
	Mantener interlocución frecuente con el proveedor afectado para conocer la evolución del incidente e identificar si surgen nuevos aspectos a considerar (cambio en el nivel de peligrosidad, nuevos IoCs, etc.).	
Medidas especiales de Monitorización	Monitorizar los IOC detectados y hacer un seguimiento de los mismos.	Departamento de seguridad de la Entidad - CERT.
	Reforzar la revisión del SIEM y la actividad de la red en búsqueda de anomalías que puedan evidenciar un incidente de Seguridad.	

ETAPA 5

Recuperación del Servicio

TAREAS	RESPONSABLE
Entrega de Informe de los equipos y de las personas: certificado que acredite qué personas y equipos del proveedor van a tener acceso a la red de la Entidad, indicando entre otra información: • Nombre de la persona. • Lugar de trabajo. • Responsable del equipo. • Sociedad en la que presta servicio. • Equipo. • Versión del sistema operativo. • MAC del equipo. • Nombre del equipo. • Actualización realizada. • Confirmación de equipo limpio. Además, debe asegurar que el Usuario no dispone de permisos de administración sobre su equipo.	
Entrega de certificado garantizando que los equipos han sido revisados, disponen de antivirus actualizado, y especificando el Sistema Operativo del que disponen.	→ Responsable de Seguridad del proveedor.
Entrega de Certificado del Responsable de Seguridad del Proveedor garantizando que todo el personal del proveedor que presta el servicio en las instalaciones de la Entidad ha recibido formación en ciberseguridad.	
Informar al Comité de Seguridad, crisis o dirección , según corresponda, para evaluar y tomar la decisión de readmisión de tráficos y conexiones. La decisión puede ser parcial.	
Verificar que los equipos que se conecten a la red de la Entidad estén en un segmento de red limpio, para volver a establecer el túnel IPSEC .	→ Departamento de seguridad de la Entidad - CERT/SOC y Responsable de Seguridad del proveedor.
Verificar que el tráfico es limpio y no se detecta ninguna anomalía.	
Activar tarjetas de acceso para los usuarios del proveedor.	→ Departamento de Servicios Generales de la Entidad.
Revisar toda la documentación referenciada para dar su conformidad y autorización a los Departamentos correspondientes para el desbloqueo de las medidas adoptadas.	
Emitir autorización expresa para la reincorporación del personal a las instalaciones de la Entidad.	→ Departamento de seguridad de la Entidad.

ETAPA 6

Cierre de Incidente

TAREAS	RESPONSABLE
Elaboración informe detallado del incidente, en el que se especifique: • El vector de entrada del incidente. • IOCs (Indicadores de compromiso). • Fecha de origen del incidente. • Acciones de remediación que se han tomado.	El Responsable de Seguridad del proveedor.
Entregar un certificado que asegure que ninguno de los equipos que se han conectado a las redes y sistemas de información de la Entidad han estado afectados por el incidente.	
Entregar plan de acción.	
Realizar los informes de cierre. Por ejemplo: • Técnico Interno, incluyendo lecciones aprendidas. • Técnico externo para Autoridades de control (cierre), si corresponde. • Ejecutivo interno, incluyendo resumen de lecciones aprendidas / mejoras abordadas.	El Responsable de Seguridad de la Entidad.

V. INVOLUCRADOS

Proveedor del Servicio

- Debe enviar una notificación desde el Departamento de Seguridad donde se indique que se está sufriendo un incidente de seguridad en los equipos y sistemas, y de qué clase de incidente de seguridad se trata.
- En caso de que el incidente haya sido notificado al Entidad por otra vía (CERT, SOC, prensa…), debe confirmar si están sufriendo el incidente o no.
- Debe identificar al Responsable de Seguridad del proveedor, que figurará como persona de contacto del proveedor para la Entidad, y será el Responsable de entregar los certificados pertinentes y llevar a cabo las acciones necesarias por parte del Proveedor del Servicio.

Responsable de Seguridad del Proveedor

- Debe ser informado de cualquier anomalía relacionada con el incidente.
- Debe conocer el punto de contacto de Seguridad de la Entidad (CISO, CERT, SOC,etc.).
- Debe entregar un Certificado que acredite qué personas y equipos del Proveedor del servicio van a tener acceso a la red de la Entidad (si no se ha entregado previo al incidente se deberá notificar quién tiene acceso en ese momento).
- Debe entregar un Certificado garantizando que los equipos han sido revisados, disponen de antivirus actualizado, y especificando el Sistema Operativo del que disponen.
- Debe entregar un Certificado garantizando que todo el personal del Proveedor que presta el servicio en las instalaciones de la Entidad ha recibido formación en ciberseguridad.
- Debe verificar que una vez reestablecido el túnel IPSEC el tráfico es limpio y no se detecta ninguna anomalía.
- Debe facilitar a la Entidad un informe detallado del incidente, en el que se especifique:

  o El vector de entrada del incidente.
  o IOCs.
  o Fecha de origen del incidente.
  o Acciones de remediación que se han tomado.

- Debe aportar un certificado que asegure que ninguno de los equipos que se han conectado a las redes y sistemas de información de la Entidad han estado infectados por el incidente.
- Debe entregar el plan de acción.

CERT/SOC INTERNO

- Debe investigar cualquier síntoma de alteración en el flujo de comunicación de los Sistemas de Información de la Entidad.
- Debe exponer las medidas de seguridad que es necesario aplicar en cada momento para la gestión del Incidente de Seguridad.
- Debe Identificar los mecanismos de comunicación que tienen conexión entre la Entidad y el proveedor afectado (túneles IPSEC y VPN, etc).
- Debe realizar un informe detallado del incidente. Este informe será contrastado con el aportado por el Proveedor del Servicio.
- Debe registrar toda la información del incidente en la plataforma de gestión de incidentes (RTIR).
- Debe verificar que las medidas solicitadas por el área responsable de Ciberseguridad han sido aplicadas, cumplen su objetivo y los bloqueos han sido exitosos, y para ello debe:

  o Verificar que no existe tráfico en los túneles IPSEC en ambas direcciones.
  o Comprobar que los usuarios permanecen bloqueados en la Gestión de la Identidad, directorio activo, etc.
  o Monitorizar los IOC detectados y hacer un seguimiento de los mismos.
  o Comprobar diariamente las MTAs (servidores de correos) entrantes para verificar el bloqueo de las direcciones de correo.
  o Verificar el bloqueo de los usuarios del proveedor en la NAC de la Entidad.
  o Reforzar la revisión del SIEM y la actividad de la red en búsqueda de anomalías que puedan evidenciar un incidente de Seguridad.

Persona o personas de La Entidad Responsable del Proveedor

- Para cada uno de los servicios objeto del contrato en los que el proveedor proporcione actividad, debe entregar un listado al Área Responsable de Ciberseguridad, con las personas que forman parte del mismo.

Área Responsable de Ciberseguridad

- Debe notificar al Comité de Seguridad, de Crisis, etc, los avances, medidas y repercusión del Incidente, según los tiempos establecidos.
- Debe valorar si es necesario elevar al Comité de Crisis la comunicación del Incidente.
- Debe solicitar las siguientes medidas, a través del sistema de ticketing o equivalente:

  o Debe solicitar cortar el tráfico de los túneles IPSEC en ambas direcciones.
  o Debe solicitar el bloqueo de los usuarios en la Gestión de Identidad, con lo que asimismo se consigue bloquear el acceso por VPN.
  o Bloquear los indicadores de compromiso (IOC) que se reciban de CERTs de referencia acreditados, SOC, etc. y del propio proveedor.
  o Debe solicitar el bloqueo del correo entrante de los dominios del Proveedor del Servicio en las MTAs (servidores de correos).
  o Debe solicitar dar de baja los usuarios del Proveedor afectado de la NAC de la Entidad.
  o Debe solicitar impedir el acceso físico a las instalaciones de la Entidad a los usuarios del Proveedor del Servicio afectado.
  o Debe solicitar nuevamente la habilitación de las tarjetas de acceso a las instalaciones de la Entidad.

- Debe revisar la documentación entregada por el Responsable de Seguridad del Proveedor para la recuperación de la normal prestación del servicio, y dar su conformidad y autorización para el desbloqueo de las medidas adoptadas.
- Si procede, debe contactar e informar a las autoridades de control.
- Debe realizar los informes de cierre.
- Evaluar, en función de la peligrosidad del incidente en proveedor, si procede la comunicación proactiva de dicho incidente y de las medidas principales adoptadas por la Entidad a stakeholders clave.

Responsable de Seguridad de la Entidad, o de la Sociedad correspondiente en su caso

- Debe dar su autorización para la reincorporación del personal a las instalaciones de la Entidad.

Área de Comunicaciones

- Debe cortar el tráfico de los túneles IPSEC en ambas direcciones, solicitado por el Área Responsable de Ciberseguridad.

- Una vez resuelto el incidente, tras la solicitud de el Área Responsable de Ciberseguridad, debe habilitar de nuevo el tráfico de los túneles IPSEC en ambas direcciones, habilitando para ello un segmento de red limpio.

Área de Infraestructura de Seguridad

- Debe verificar que las personas que constan en las herramientas de las que dispone la Entidad (Gestión de Identidad y Directorio Activo), coinciden con el listado entregado por la Persona de la Entidad Responsable del Proveedor.

- Debe bloquear los usuarios en la Gestión de IdEntidad, que ha solicitado el Área Responsable de Ciberseguridad.

- Dependiendo del tipo de IPS del que se haya solicitado el bloqueo por el Área Responsable de Ciberseguridad, debe bloquear el mismo en:

  o Firewall.
  o Proxy.
  o Antimalware.
  o IPSs.

- Debe dar de baja a los usuarios del Proveedor afectado, solicitado por el Área Responsable de Ciberseguridad, de la NAC de la Entidad.

- Una vez resuelto el incidente, y con la autorización del Área responsable de Ciberseguridad, debe desbloquear los usuarios en la Gestión de IdEntidad, directorio activo, etc.

- Una vez resuelto el incidente, y con la autorización del Área Responsable de Ciberseguridad, debe dar de alta de nuevo a los usuarios del Proveedor afectado en la NAC de la Entidad.

Área de Sistemas (Responsable de los sistemas de correo)

- Debe bloquear el correo entrante, solicitado por el Área Responsable de Ciberseguridad, de los dominios del proveedor del servicio en las MTAs (servidores de correos).
- Una vez resuelto el incidente, y con la autorización de el Área Responsable de Ciberseguridad, debe desbloquear el correo entrante de los dominios del proveedor del servicio en las MTAs (servidores de correos).

Área responsable del control de acceso físico a las instalaciones de la organización

- Tras la petición del Área Responsable de Ciberseguridad de impedir el acceso físico a las instalaciones del personal de proveedor afectado, debe deshabilitar la tarjeta de acceso a las instalaciones.
- Debe habilitar de nuevo la tarjeta de acceso a las instalaciones, una vez sea solicitado por el Área Responsable de Ciberseguridad.

VI. GLOSARIO

SIEM (Security Information and Event Management,): Un sistema SIEM recopila los eventos de seguridad que se generan en los sistemas de seguridad y de información, los correlaciona , aportando trazabilidad y mediante su análisis genera una nueva información más rica que los eventos aislados, pudiendo identificar incidentes y/o generando alertas.

RTIR (Request Tracker for Incident Response): Es una aplicación que responde a las necesidades de documentación, asignación, tratamiento y gestión de los equipos de respuesta a incidentes.

NAC (Network Access Control): es una tecnología que permite controlar de forma muy granular qué dispositivos pueden acceder a la red, permitiendo establecer políticas de gestión de acceso de los dispositivos a la red cableada, móvil o wifi), pudiendo solicitar credenciales, MACs o certificados digitales como mecanismos de autenticación u explorando otras características del equipo tales como el sistema operativo o si tienen antimalware o no.

GID (Gestión de la Identidad). La gestión se ejerce sobre todo el ciclo de vida de la identidad y de las credenciales de la misma. El sistema suele contar con un directorio en el que se autentican las identidades.

IPSEC (abreviatura de Internet Protocol security): es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. Los túneles IPSEC, suelen unir sedes, dotando de un canal seguro entre las mismas.

IPS ((Intrusion Prevention System): Un sistema de prevención de intrusos es un software que inspecciona el tráfico de una red informática para proteger a los sistemas de información de ataques conocidos. Usualmente se basan en firmas y reputación.

Más información en:

isms forum

www.ismsforum.es