

Telefónica Móviles España: Sistema de Gestión Integral de Eventos de Seguridad

La implantación de un Sistema de Gestión Integral de Eventos de Seguridad debe estar alineada con la estrategia de seguridad de la compañía, apoyándose en tres pilares fundamentales: Políticas de Seguridad, Organización, y Proceso y Herramientas Técnicas. La Gerencia de Seguridad Informática de la Dirección General de Sistemas de Información de Telefónica Móviles de España decidió abordar este problema implantando la solución GEMA del Grupo SIA.



José María Conde / Félix Gallego

A menudo se pierde de vista el objetivo de la seguridad de SS.II.: proteger el valor del negocio. Al planificar la estrategia de seguridad se ha de tener en cuenta que debe existir una adecuación e integración de la seguridad total con los procesos de negocio a los que se da soporte. En la Gerencia de Seguridad Informática de la Dirección General de Sistemas de Información de Telefónica Móviles España, el concepto de seguridad está soportado por tres columnas fundamentales, Políticas de Seguridad, Organización y Proceso y Herramientas técnicas. Son estos tres pilares y sus relaciones entre sí los que dotan a la seguridad de los cimientos para poder proteger el negocio.

El modelo de seguridad

Teniendo en cuenta estos tres pilares, el Modelo de Seguridad se plantea como un ciclo de mejora continuo, mediante fases de diseño, operación y revisión. Primero se diseña la estrategia de actuación en base a requisitos de negocio, políticas y necesidades organizativas. Después se procede a la operación de la solución, explotando las soluciones técnicas y, por último, se revisan los resultados para afinar el diseño, cerrando de este modo el proceso de mejora continua.

La base metodológica que soporta se define de forma piramidal, concretándose a medida que se alcanzan los niveles inferiores. En el nivel superior de la pirámide se encuentra la Política de Seguridad global, que se particulariza progresivamente en Normativas, Estándares y Guías hasta llegar a un nivel de detalle óptimo en el

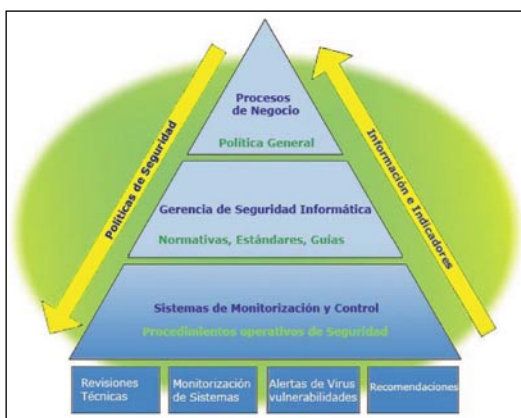


Figura 1. Visión de la seguridad orientada al soporte de los procesos de negocio.

que se encuentran los *Procedimientos Operativos de Seguridad*.

Estos *Procedimientos Operativos* son llevados a la práctica por los sistemas finales de Detección y Control de Eventos mediante reglas de gestión implementadas en las *Herramientas técnicas*.

Cada una de las reglas (más de 100) que se implanta en el sistema de monitorización, cada política de acceso que se gestiona en los sistemas, cada uso de un recurso que se monitoriza, cada mecanismo de revisión de los servicios prestados al negocio, vienen avalados por la *Política de Seguridad* y descritos en detalle en los *Procedimientos Operativos de Seguridad*.

Sistema de Gestión Integral de Eventos de Seguridad

¿Cómo se reducen 20 millones de eventos de seguridad monitorizados al año a 7.000 tickets reales gestionados que aplican en la compañía? ¿Cómo se

gestionan más de 200 sistemas en producción? ¿Cómo se monitoriza el uso de recursos de más de 8.000 puestos de usuario?

Telefónica Móviles España ha apostado por la solución GEMA del Grupo SIA para implementar su Sistema de Gestión Integral de Eventos de Seguridad. GEMA consta de módulos de *Detección, Control y Gestión de los Eventos de Seguridad*, que permiten la automatización de procesos de filtrado de información y la gestión de la información resultante por los consultores de seguridad.

La base para la reducción progresiva del volumen de incidencias a tratar es la gestión, correlación y filtrado de los eventos detectados, comenzando por una correcta implementación de las reglas de negocio especificadas en los *Procedimientos Operativos*.

Por ejemplo, si la política de seguridad define que las credenciales de acceso a recursos de los usuarios son intransferibles, se monitorizarán los accesos desde diferentes direcciones, tramos horarios y segmentos de red para detectar patrones anómalos.

GEMA permite la implementación de las reglas de negocio especificadas en los *Procedimientos Operativos* en cada uno de sus módulos de *Detección*.

Los módulos de detección comprenden tanto la detección activa, basada en *Monitorización* de sistemas y *Revisiones Técnicas*, como la detección preventiva mediante la recepción de *Avisos de Alertas Tempranas de Vulnerabilidades y Virus*, y la *Gestión de las Recomendaciones de Seguridad* emitidas por los fabricantes (el 99% de los ataques provienen de la explotación de vulnerabilidades conocidas).

De esta forma, uniendo la potencia de la detección activa y preventiva de eventos, GEMA permite "poner ojos en la red" y conseguir la imagen completa del estado de seguridad de los sistemas e infraestructuras.

Los eventos hallados mediante los módulos de detección son procesados por un motor de lectura que los normaliza y los convierte en *Tickets de Seguridad*. La información de estos tickets resultantes es completada con datos relativos a los activos a los que afectan, con el fin de poder aportarles información de calidad relacionada con el negocio, sobre criticidades, valor e impacto de los activos afectados. Este proceso de *mapeo* de los sucesos detectados con los activos reales permite un segundo nivel de eliminación de falsos

positivos y una mayor concreción en la información que se reporta a los consultores de seguridad.

Mediante estos procesos automáticos se consigue que sólo la información realmente importante llegue finalmente a una consola de gestión centralizada.

La Consola de Gestión de Tickets de Seguridad permite trasladar los eventos filtrados y ponderados a los consultores de seguridad para su tratamiento y gestión. En la consola los consultores procesan los *tickets*, resolviendo, asumiendo o delegando la resolución de los mismos.

Así mismo, la consola de seguridad permite la gestión centralizada y el *trabajo colaborativo* entre los múltiples roles (operadores, técnicos de sistemas, consultores) que intervienen en la resolución de un *ticket*, convirtiéndose en un punto de encuentro que garantiza la independencia entre administradores de sistemas, consultores de seguridad y responsables de los activos. Además, permite el almacenamiento y gestión de toda la información relacionada con la detección de eventos para ayudar en los posibles *procesos forenses* posteriores.

Una de las tareas más importantes de gestión de los consultores con la Consola de Seguridad es la comunicación de los *tickets* a los *flujos de trabajo corporativos* para su resolución, así como la notificación de *comportamientos incorrectos* a los *usuarios finales*. Mediante esta comunicación a las capas superiores, se cierra el ciclo de integración de la seguridad en el negocio.

La notificación continua de los *tickets* de seguridad a los usuarios finales ofrece además beneficios añadidos a los procesos de concienciación, entre otros, poner ojos en lo que está pasando en la red, dirigir esfuerzos de análisis en lo que consideramos importante, capacidad de reacción rápida y coordinación de grupos, y mecanismo de concienciación de seguridad de los usuarios y responsables con datos concretos sobre el no cumplimiento de la política de seguridad o riesgo de seguridad.

La solución aquí tratada, permite mostrar indicadores de los procesos de Gestión Integral de Eventos de Seguridad,

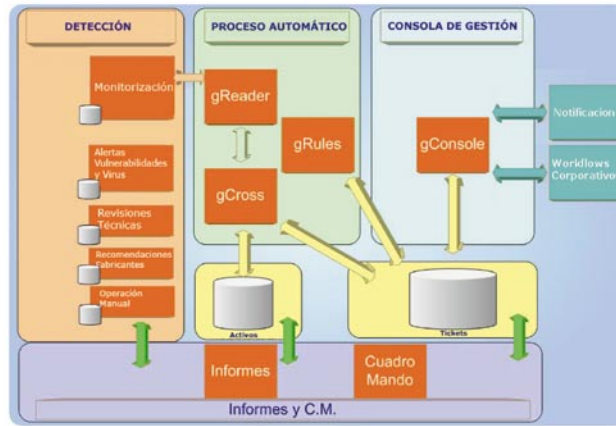


Figura 2. Diagrama de módulos de la solución GEMA

cuyo objetivo es obtener el estado de la seguridad de los sistemas.

Dichos indicadores proporcionan información sobre el grado de *cumplimiento de las políticas de seguridad*, basados en *umbrales de referencia* obtenidos tras la operación continua (*clipping-levels*).

Los valores obtenidos de la operación, en comparación con los niveles de referencia de fases previas, constituyen la mejor forma de evaluación para detectar la efectividad de las medidas implantadas y los proyectos abordados en un periodo determinado.

Sistema de *Gestión Integral de Eventos de Seguridad*, tanto de negocio como tecnológicos.

En el caso específico de GEMA, la aportación al negocio se concreta en la aportación de una visión global sobre la seguridad, que apoya a la toma de decisiones; una información de calidad para determinar el retorno de la inversión, que facilita la preparación de nuevos planes estratégicos; una reducción de costes en comparación a un análisis manual y no centralizado; agilidad y rapidez de respuesta, y una reducción de riesgos (incidentes de seguridad).

Desde un punto de vista tecnológico, los beneficios se centran en la existencia de una seguridad activa y preventiva ante eventos de seguridad; una centralización de la operación en una Consola de Gestión de Tickets; una respuesta rápida ante ataques; la integración de los eventos de seguridad en los *workflows* corporativos, y la notificación directa a usuarios de usos no adecuados.

Además, existen unos beneficios indirectos, que son aquellos que aunque intangibles en una primera aproximación, aportan un valor añadido a la solución, como son la involucración de toda la compañía en la política de seguridad, la ayuda en la concienciación de seguridad a todos los niveles y la ayuda en la justificación de las actuaciones de seguridad en base a su efectividad.

Telefónica Móviles España, tras varios años de explotación de su sistema de Gestión de Seguridad, esta alcanzando un alto grado de madurez en la conciliación de políticas de negocio y sus proyectos de seguridad, sacando el máximo partido a la Gestión de la Seguridad apoyada en la solución aportada por el Grupo SIA. ■

Código	Fuente	Título	Aplica	Críticidad	Fecha	Tickete Asoc.
T1006-010843	0E-000002	SAC Acceso del mismo usuario desde diferentes IPs	SI	000 4	15/07/2005 01:48:58	14
T1006-010871	0E-000021	FAS Intentos de login de diferentes usuarios/interno equipo	SI	000 5	15/07/2005 01:48:24	4
T1006-010842	0E-000000	FAS Acceso desde misma IP distintos usuarios	SI	000 4	15/07/2005 01:26:11	8
T1006-010852	0E-000000	SAC Acceso desde misma IP distintos usuarios	SI	000 4	15/07/2005 01:21:26	7
T1006-010851	0E-000000	MSF Integroplog sistema de serv. iava	SI	000 4	15/07/2005 01:08:52	13
T1006-010853	0E-000000	FAS Acceso desde misma IP distintos usuarios	SI	000 4	15/07/2005 01:01:09	10
T1006-011004	0E-000000	SAC Num. Exceso de intentos de acceso - usuario	SI	000 4	15/07/2005 00:24:32	1
T1006-011002	0E-000000	FW1 Búsqueda de puertos vulnerables	SI	000 4	15/07/2005 00:14:33	1
T1006-011003	0E-000000	FW1 Búsqueda de puertos vulnerables	SI	000 4	15/07/2005 00:14:31	1
T1006-011001	0E-000000	FW1 Búsqueda de puertos vulnerables	SI	000 4	15/07/2005 00:14:27	1
T1006-011000	0E-000000	FW1 Búsqueda de puertos vulnerables	SI	000 4	15/07/2005 00:14:26	1
T1006-000254	MCID 0017	W32.Pobut.PDF@msn	SI	000 4	15/07/2005 04:18:06	1
T1006-000253	MCID 0016	W32.Pobut.A	NO	000 0	15/07/2005 04:18:07	1
T1006-000393	0E-000000	Macromedia Run Unauthorized Session Access Vulnerability	NO	000 4	15/07/2005 04:18:14	1
T1006-000392	0E-000000	Sophos Anti-virus 0202 Archive handling remote Denial Of Service Vulnerability	NO	000 5	15/07/2005 04:18:11	1

Figura 3. Consola de Gestión de Tickets de Seguridad

Estos indicadores se agrupan en un Cuadro de Mando de operación, perfilado según los roles a los que van dirigidos, que permite el apoyo a la toma de decisiones a todos los niveles. En base a dichos indicadores, se pueden elaborar los planes de actuación para siguientes campañas, centrando el foco en aquellos puntos en los que la seguridad necesite mayor atención y compromiso.

GEMA

Existen unos beneficios directos que se derivan de la implantación en sí de un

JOSÉ MARÍA CONDE
Gerente de Seguridad Informática
TELEFÓNICA MÓVILES ESPAÑA

FÉLIX GALLEGO
Responsable de Proyecto
Grupo SIA
fgallego@sia.es