Impacto en recursos y presupuesto en el despliegue de las medidas de protección del ENS

Javier Zubieta Moreno
Responsable de Desarrollo de Negocio de Seguridad
jzubieta@gmv.com

Secure e-Solutions®
GMV SOLUCIONES GLOBALES INTERNET S.A.

INFORMACIÓN CONFIDENCIAL

El presente documento ha sido clasificado como "Información Confidencial" dentro del marco del Sistema de Gestión de la Seguridad de la Información (SGSI) de GMV-SGI. Dicha clasificación habilita a su receptor al uso de la información contenida en el documento para los fines para los que GMV-SGI la ha facilitado o a lo acordado contractualmente con relación al intercambio de información, en su caso, entre las partes, y ello sin perjuicio del cumplimiento de la normativa sobre propiedad intelectual y sobre protección de datos de carácter personal.

gmv® INNOVATING SOLUTIONS

Contexto

 © GMV, 2012

Introducción

- Con los Planes de Adecuación ya elaborados, es momento de desarrollar el ENS a través de las Medidas de Seguridad, detalladas en el Anexo II del mismo

- Esta presentación recopila los probables subproyectos que desencadena el cumplimiento del ENS y cataloga su impacto en alto, medio o bajo atendiendo a:
  - Presupuesto necesario
  - Recursos humanos
  - Tiempo dedicado

Proyectos y Servicios a considerar

- Proyectos de consultoría
- Proyectos de despliegue de soluciones tecnológicas para las Medidas de Protección, incluyendo instalación, integración, soporte y mantenimiento
- Servicios gestionados: Niveles de Servicio, Monitorización y soporte a la Gestión de Incidentes
- Oficina de Seguridad enfocada a ENS+ENI
- Seguimiento y control basado en herramientas de gestión ENS

Marco Organizativo
[org] Proyectos aplicables

Planteamiento general

- Se trata de trabajos de consultoría con un entregable bien definido: documentación
- Este tipo de trabajos se suele abordar con proyectos puntuales o bien dentro de una Oficina de Seguridad
- Todos los entregables pueden ser el resultado de una única Consultoría

Recomendaciones

- Política corta en longitud
- Procedimientos detallados

© GMV, 2012

Marco Operacional – Planificación
[op.pl] Proyectos aplicables

Planteamiento general

- Se trata de trabajos de consultoría con un entregable bien definido: documentación
- Este tipo de trabajos se suele abordar con proyectos puntuales de definición o revisión, o bien dentro de una Oficina de Seguridad
- Muchos entregables requieren aprobación por la Dirección en categorías media y alta

Recomendaciones

- Reutilización y revisión de lo existente: Análisis de Riesgos y Arquitecturas de seguridad
- El alcance es determinante

© GMV, 2012

Marco Operacional – Control de acceso
[op.acc] Proyectos aplicables

Planteamiento general

- Se trata de un mix de consultorías de definición (perfilado de usuarios, provisioning, procedimientos de altas/bajas, etc) con la implantación efectiva de medidas tipo IAM
- Este tipo de trabajos se suele abordar con proyectos puntuales de definición o revisión, con proyectos de integración o bien dentro de una Oficina de Seguridad

Recomendaciones

- Revisión del IAM existente en la organización
- Centralización de las autorizaciones de distintos departamentos: sistemas, comunicaciones, aplicaciones, desarrollo, etc

© GMV, 2012

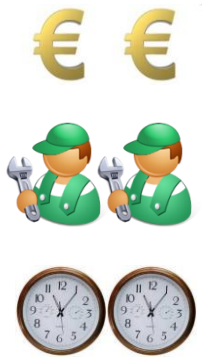
Marco Operacional – Explotación
[op.exp] Proyectos aplicables

Planteamiento general

- La componente tecnológica es más acusada
- Entran en juego también los Servicios Gestionados, además de los anteriormente mencionados

Recomendaciones

- Tender hacia un servicio mezcla de servicios externalizados remotos e insitu y proyectos puntuales
- Adoptar buenas prácticas de estándares tipo ISO20000



 © GMV, 2012

Marco Operacional – Servicios externos
[op.ext] Servicios aplicables

Planteamiento general

- Aparte de las consultorías de definición necesarias, este tipo de trabajos se suele abordar dentro de una Oficina de Seguridad
- Para la medida *op.ext.1 Contratación y acuerdos de nivel de servicio*, será necesario la coordinación con el departamento legal o el de contratación

© GMV, 2012

Marco Operacional – Continuidad del servicio
[op.cont] Proyectos aplicables

Planteamiento general

- Se trata de trabajos de consultoría con un entregable bien definido: documentación
- La existencia del Plan de Continuidad es obligatoria, pero más importante es la aplicación práctica del mismo
- Sistema de Gestión de Continuidad de Negocio

Recomendaciones

- Bajo el paraguas del SGCN se cobijan todos los requisitos del ENS y muchos más
- El prestador de servicios debería estar certificado (UNE 71599, BS)

Marco Operacional – Monitorización del sistema
[op.mon] Proyectos aplicables

Planteamiento general

- El ENS lo restringe a Categoría Alta y a herramientas de IDS / IPS
- Se puede hacer un planteamiento más ambicioso, con disponibilidad, eventos de seguridad, vulnerabilidades, etc
- Pueden entrar en juego también los Servicios Gestionados

Recomendaciones

- Acometerlo mediante Servicios Gestionados si es factible
- Integrar sistemas de monitorización ya existentes (sobre todo disponibilidad)
- Plantear alquiler de equipamiento

 © GMV, 2012

Contexto

 © GMV, 2012

Medidas de protección – Protección de las instalaciones y la infraestructura
[mp.if] Proyectos aplicables

Planteamiento general

- Parte de las medidas aparecen en un SGCN y en un SGSI
- Especialmente impactante la medida mp.if.9. Instalaciones alternativas (nivel Alto)
- Enlace con la LOPD en la *mp.if.2. Identificación de las personas* y en la *mp.if.7. Registro de entrada y salida de equipamiento*

Recomendaciones

- Procedimentar la interacción con Seguridad Física (mundos separados)
- Aprovechar al máximo los controles de los SGCN y SGSI si hubiere

Medidas de protección – Gestión del personal
[mp.per] Proyectos aplicables

Planteamiento general

- Aparte de las consultorías de definición necesarias, este tipo de trabajos se suele abordar dentro de una Oficina de Seguridad y con acciones concretas (concienciación y formación)
- Muchas similitudes con el apartado *A.8, Seguridad del personal*, de la ISO 27001

Recomendaciones

- Implementación efectiva por parte de RRHH, líderes de esta Medida

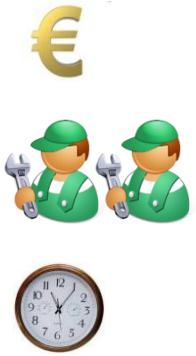
Medidas de protección – Protección de los equipos
[mp.eq] Proyectos aplicables

Planteamiento general

- Se acometería mediante consultorías de definición e instalación de medidas de protección concretas para la *mp.eq.3. Protección de puesto de trabajo*
- Desde el punto de vista tecnológico, se suele abordar como un proyecto dentro de una estrategia DLP

Recomendaciones

- Procedimentar la interacción con Seguridad Física (mundos separados)
- Ampliar las medidas de protección de portátiles del ENS a otras relacionadas, como control de puertos, escritorio seguro, etc
- Consumerization – BYOD (!!!)



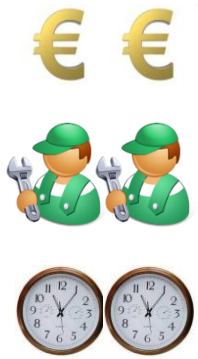
Medidas de protección – Protección de las comunicaciones
[mp.com] Proyectos aplicables

Planteamiento general

- En general se trata de proyectos de integración de soluciones de seguridad para las comunicaciones, con el estudio de definición de arquitecturas y de segmentación de redes
- Abarca las medidas de protección más clásicas en las organizaciones, aunque también las más obsoletas
- Una revisión de configuraciones resulta imprescindible

Recomendaciones

- Verificar la vigencia de vida y soporte del equipamiento actual
- Revisar y optimizar las configuraciones existentes. La máxima "si funciona no lo toques" no es válida
- Monitorizar la disponibilidad del servicio



 © GMV, 2012

Medidas de protección – Protección de los soportes de información

[mp.si] Proyectos aplicables

Planteamiento general

- Se necesita, por un lado, la definición de las medidas y los protocolos de actuación (los procedimientos del marco organizativo)
- Y por otro lado, la correcta transmisión de la información y concienciación, dado que la efectividad de las medidas depende casi completamente de las personas

Recomendaciones

- Concienciación, a varios niveles, tipología variada de personal
- Papel ¿?

Medidas de protección – Protección de las aplicaciones informáticas
[mp.sw] Proyectos aplicables

Planteamiento general

- La seguridad en el desarrollo se suele abordar a 3 niveles:
  - La definición de las metodologías de desarrollo seguro
  - Las pruebas de conformidad de seguridad de la aplicación que se desarrolla
  - Las soluciones tecnológicas que implementan medidas de protección específicas (firewalls de aplicación web)

Recomendaciones

- Combinar distintas metodologías y buenas prácticas (OWASP, OpenSAMM, WASC, …)
- Realizar pruebas en entorno pre y post producción
- No descuidar el fw de aplicación

Medidas de protección – Protección de la información
[mp.info] Proyectos aplicables

Planteamiento general

- Se acometería mediante consultorías de definición, instalación de medidas de protección concretas e integración con servicios comunes, como Verificación de firmas y Sellado de tiempo
- Complejidad alta de implantación de medidas de seguridad en función de la calificación de la información

Recomendaciones

- Compromiso de mínimos en la implantación de medidas de protección según la calificación de la información
- Utilizar al máximo los servicios ya existentes

 © GMV, 2012

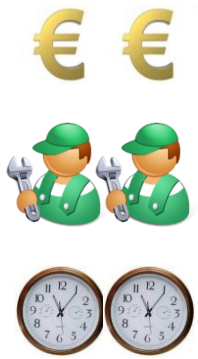
Medidas de protección – Protección de los servicios
[mp.s] Proyectos aplicables

Planteamiento general

- Se acometería mediante integración de soluciones tecnológicas
- Debería tener en cuenta la medida de Calificación de la Información
- Tendencia de mercado: atentos a los Cloud Services, encajan bien aquí
- La *mp.s.3. Protección frente a denegación de servicio*, es crítica: puede que salgas en los medios de comunicación

Recomendaciones

- La *mp.s.1. Protección del correo electrónico*, es muy probable que esté implantada, sólo habría que revisarlo o replantearlo
- La *mp.s.2. Protección de servicios* y aplicaciones web, apunta a un Fw de aplicación web, por ahora tenerlo inhouse



Conclusiones

Gracias

Javier Zubieta

Responsable de Desarrollo de Negocio de Seguridad de la Información

jzubieta@gmv.com

www.gmv.com

INNOVATING SOLUTIONS