



BUSINESS INFORMATION[®] CHECKUP

Assessing Corporate Information Security

La realización del **Business Information Check-Up[®]** o Análisis de Riesgos de Alta Penetración proporciona al cliente una lista detallada de vulnerabilidades en torno a la información contenida dentro y fuera de sus sistemas de información, estableciendo en cada caso el nivel de riesgo.

En dicho Análisis no solo mostramos los hallazgos y vulnerabilidades a nivel técnico. A través de generar patrones de posibles ataques al crear escenarios de explotación sobre conjuntos de vulnerabilidades encontradas, GCP Global busca demostrar que tan profundo se podría llegar a penetrar dentro de una organización a partir del aprovechamiento sistemático de varios de los huecos que quizá por si solos, no representan una gran amenaza para la continuidad del negocio. Esto permite a la organización que aplique el análisis, establecer un correcto orden de prioridades en la implementación de parches y soluciones, ya sean temporales o permanentes.

En un tiempo reducido, se conoce el estado actual de riesgo de la información corporativa, analizando: redes, comunicaciones, aplicaciones críticas, bases de datos, seguridad física, además de revisar las prácticas en el manejo de la información por parte de los usuarios y verificar tanto la existencia como la aplicación de políticas y procedimientos relacionadas al manejo seguro de la información.

Dicho diagnóstico sirve para contrastar las condiciones prevalecientes en la seguridad de la información contra los más reconocidos estándares de seguridad de Tecnologías de la Información existentes.

De acuerdo con la profundidad del Análisis de Riesgos, los resultados son organizados por capas, conforme al Modelo de Seguridad Integral ilustrado en la *figura 1*.

El análisis construye las bases para la definición de la Estrategia de Seguridad Corporativa y las sugerencias de cómo aminorar los riesgos de la seguridad, basados en las necesidades específicas del negocio.

Entregables:

- Dictamen de Seguridad de Información
- Resumen de vulnerabilidades y riesgos representativos
- Conclusiones
- Recomendaciones Generales
- Plan de acción Sugerido
- Detalle de vulnerabilidades y riesgos
- Resumen Ejecutivo



Presencia de Seguridad:

Medio ambiente (entorno) encontrado al mismo nivel físico ó lógico dentro de una evaluación de Seguridad.

Dentro de cada "Presencia de Seguridad" existen elementos que a su vez pueden existir dentro de otras "Presencias de Seguridad" y que de acuerdo a la metodología OSSTMM estos elementos deberán ser a su vez verificados como parte integral de una evaluación de seguridad.

De acuerdo a normativas internacionales para que una prueba de seguridad sea completa, ésta debe de contemplar la evaluación en cuatro dimensiones fundamentales, que son:

- a) **Visibilidad.** Enumeración de todo aquello que puede ser visto acerca de la "Presencia de Seguridad".
- b) **Acceso.** El porqué las personas entran a la "Presencia de Seguridad".
- c) **Confianza.** Aquellos sistemas o relaciones complejas que existen dentro de la "Presencia de Seguridad".
- d) **Alarma.** Aquellas reacciones predeterminadas existentes para visibilidad, acceso y confianza.

La seguridad de los elementos analizados dentro de cada "Presencia de Seguridad" se contrasta con el modelo de seguridad denominado "Seguridad Perfecta", que define el "deber ser" en términos de seguridad.

El proceso de evaluación de seguridad a través de las distintas "Presencias de Seguridad" involucradas en la metodología propuesta se resume en la siguiente gráfica:

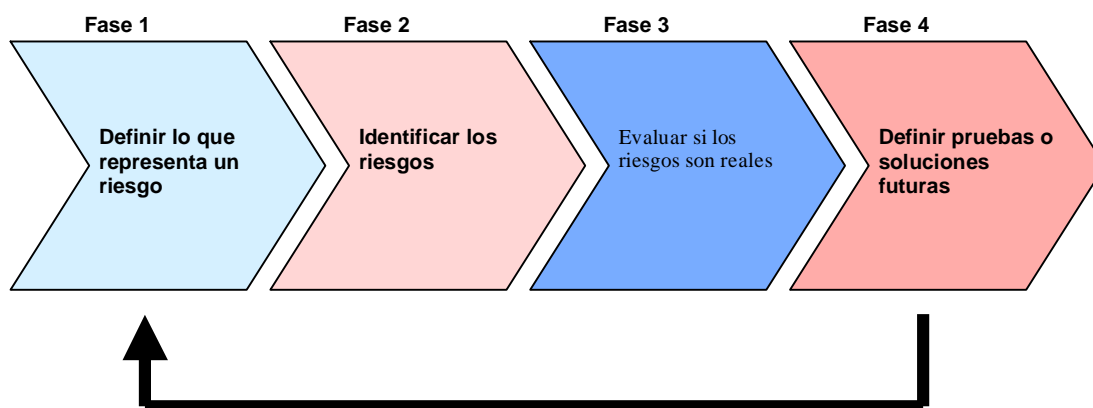


Fig. 2. Proceso de evaluación de seguridad

Las "Presencias de Seguridad" consideradas para la realización del servicio son las siguientes:

Seguridad Física

Considera la parte Física de las estructuras de Seguridad de la Organización, centrándose en forma primaria en aquellos Mecanismos de Control de Acceso a Centros de cómputo y/o áreas donde resida información sensible para el negocio.

Organización y Usuarios

Considera la parte Formal de la Seguridad a Nivel Organización, tomando en cuenta mecanismos de publicación y cumplimiento de Políticas y Procedimientos. También comprende la estructura de Seguridad a Nivel Organizacional, es decir la entidad que es responsable de la Seguridad de la Información en todas sus capas y finalmente considera a los usuarios como otro elemento de seguridad de Información abarcando tópicos de Cultura de Seguridad y Procesos de Educación.

Aplicaciones

Se refiere a los niveles de seguridad presentes en los aplicativos, considerando exclusivamente los elementos referentes a metodología y procedimientos tales como: Metodología de Control de Proyectos de TI, Metodologías de Control de Cambios, procedimientos de actualización y/o mantenimiento de aplicaciones existentes y Separación de ambientes de desarrollo y pruebas.

Redes y Comunicaciones

La protección de la información en su entorno lógico es prioridad para el manejo eficiente y seguro de las transacciones.

La confidencialidad de la seguridad de la empresa puede verse comprometida a través de los sistemas de mensajería, por lo que tienen que verificarse los niveles de encriptación de datos, así como las capacidades de monitoreo y acceso a información sensible. Esquemas de confidencialidad e integridad, así como las capacidades de monitoreo de intrusos y accesos no autorizados, serán evaluados a través de la existencia de herramientas de protección y esquemas de respaldo.

Bases de Datos

La seguridad en las bases de datos es complemento importante de la seguridad aplicativa ya que protege contra accesos directos realizados tanto por personal técnico como por usuarios, es por ello que el control de acceso y la integridad son principios mandatorios a establecer en este nivel de seguridad.

Otro de los puntos a considerar son las actualizaciones y la instalación de parches y actualizaciones de seguridad a las bases de datos.

Sistemas Operativos y Servidores

La seguridad en los servidores es uno de los puntos más importantes ya que en estos es donde reside información electrónica importante de la institución. Por eso hay que considerar revisar las actualizaciones e instalación de parches de seguridad, mecanismos de redundancia, respaldos y mecanismos de monitoreo.

Datos e Información

Se refiere a los grupos de documentos importantes, mismos que pueden agrupar lo relacionado a la propiedad intelectual de la empresa, se auditarán en cuanto a su acceso, copias, respaldos y cambios, identificando potenciales fugas de información.