Unidad 4. Diseño del proceso de la seguridad

DESARROLLO Y GESTIÓN DE SEGURIDAD DE REDES

Esquemas de Seguridad Informática

Políticas de Seguridad Proceso del Diseño de Políticas

De acuerdo a (Daltabuit Godás & Vázquez Gómez, 2007), hay que especificar el alcance de las políticas y los objetos de las mismas, consistentemente con la misión de seguridad previamente establecida.

Esquemas de Seguridad Informática

Las políticas promulgadas deben escribirse en párrafos que sean, cada uno por separado, implementarles mediante un mecanismo específico.

Es decir, hay que procurar pensar claramente en la conveniencia de que las políticas sean sumamente específicas, si esto se puede lograr, es deseable fragmentar las políticas por departamento o unidad de trabajo.

Pueden entonces pensarse en una jerarquía de políticas, unas con aplicabilidad general, y otras para aplicabilidad para grupos o tareas específicas..

Esquemas de Seguridad Informática

Las políticas que no cuenten con la aceptación entusiasta de los usuarios de todos los niveles serán muy difíciles de implantar.

Todos aquellos que serían afectados por las políticas deben tener la oportunidad de revisarlas y hacer comentarios antes de que se promulguen, deben contar con el apoyo total de los administradores.

Esquemas de Seguridad Informática

En esta etapa deben considerarse los mecanismos de difusión, capacitación y concientización iniciales y permanentes sobre seguridad informática.

La cultura de la organización y sus necesidades de seguridad son un factor determinante para el equipo de redacción de las políticas. El nivel del control que se establezca no debe resultar en una reducción de la productividad, pues en muchos casos los ingresos y la carrera de la persona esta designadas por su productividad. Si son demasiadas restrictivas en comparación de la cultura organizacional se violarán las políticas.

Esquemas de Seguridad Informática

Las razones que llevan la implantación de una política deben de explicarse dentro de la política misma. También debe definirse la cultura de cada política: quién, qué y cuándo.

Esquemas de Seguridad Informática

Políticas de Seguridad [Definición de Política]

La política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Esquemas de Seguridad Informática

Políticas de Seguridad [Definición de Política]

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los “dueños” y permiten adoptar una buena actitud dentro de la organización.

Esquemas de Seguridad Informática

Políticas de Seguridad Criterios de las OCDE

La OCDE considera que los elementos de las políticas son:

1) Concienciación. Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

Políticas de Seguridad Criterios de las OCDE

2) Responsabilidad. Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

3) Respuesta. Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.

4) Ética. Los participantes deben respetar los intereses legítimos de terceros.

Políticas de Seguridad Criterios de las OCDE

8) Gestión de la Seguridad. Los participantes deben adoptar una visión integral de la administración de la seguridad.

9) Reevaluación. Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Políticas de Seguridad Criterios de las OCDE

5) Democracia. La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

6) Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

7) Diseño y realización de la seguridad. Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

Políticas de Seguridad (Postura)

De acuerdo a (Daltabuit Godás & Vázquez Gómez, 2007), la confianza es el principio básico que rige el desarrollo de políticas. Lo primero es determinar quién tiene privilegios, y hay que usar el principio del mínimo privilegio posible.

Hay que tener cuidado en que tanto se confía en el personal. Se otorgan privilegios a medida que se necesitan y se requieren controles técnicos para asegurar que no se den violaciones.

Adoptar el modelo "Todo lo que no esté específicamente prohibido está permitido" o bien "Todo está prohibido excepto lo que esté específicamente permitido".

Políticas de Seguridad (Beneficios)

- Las políticas de seguridad informática muchas veces ayudan a tomar decisiones sobre otros tipos de política (propiedad intelectual, destrucción de la información, etc.).

- También son útiles al tomas decisiones sobre adquisiciones porque algunos equipos o programas no serán aceptables en términos de las políticas mientras que otras la sustentaran.

Políticas de Seguridad (Beneficios)

- Las políticas de seguridad informática deben considerarse como un documento de largo plazo, que evolucionan.
  - No contienen asuntos específicos de implementación, pero si asuntos específicos del equipo de cómputo y telecomunicaciones de la organización.
  - Probablemente serán la guía para el diseño de cambios a esos sistemas.

El desarrollo e implantación de políticas de seguridad informática es una indicación de que una organización está bien administrada y los auditores lo toman en cuenta en sus evaluaciones. Condicen a una profesionalización de la organización

Políticas de Seguridad (Algunas Políticas necesarias)

De acuerdo a (Daltabuit Godás & Vázquez Gómez, 2007), hay que considerar las siguientes políticas necesarias:

- Políticas de uso aceptable. Determina que se puede hacer con los recursos de cómputo (equipo y datos) de la organización. También determinan lo que no se puede hacer con esos recursos. Indica la responsabilidad de los usuarios en la protección de la información que manejan y en qué condiciones puede afectar o leer datos que no les pertenezca.

Políticas de Seguridad (Algunas Políticas necesarias)

- Políticas de cuentas de usuario. Determina el procedimiento que hay que seguir para adquirir privilegios de usuarios en uno o más sistemas de información y la vigencia de estos derechos.
  - Además quien tiene la autoridad de asignar estos privilegios y quienes no podrían recibir esos privilegios por causas legales.
  - Debe exhibir explícitamente los deberes y derechos de los usuarios. Se explicara cómo y cuándo se deshabilitaran las cuentas de usuarios y que se hará con la información que contenga.
  - Debe especificar claramente los detalles de los procedimientos de identificación y autenticación.

Políticas de Seguridad (Proceso del Diseño de Políticas)

Investiga sobre el Proceso del Diseño de Políticas de Seguridad en las Organizaciones y realiza una Resumen.

Fecha de entrega: 3 de febrero de 2016