

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN Y ANTECEDENTES

Cuando se habla de la seguridad informática nos referimos a que cierta información tiene prioridad o bien es importante para la empresa lo cual tenemos que cuidar y proteger para que no caiga en manos erróneas o perderla ya que es vital para la empresa.

La seguridad informática debe de tener aspectos de seguridad como la confidencialidad, integridad y disponibilidad en la información de la empresa, la organización de la información de una empresa u organización anteriormente era en documentos impresos y se almacenaban en grandes cantidades como en archivadores en los cuales tenían los datos de los clientes o proveedores de la empresa, todos los registros quedaban en papel y era un problema para su almacenaje, transporte y acceso, además de ser algo pesado al momento de la revisión de alguna información. Ahora en la actualidad toda la información de la empresa esta digitalizada lo cual reduce el espacio, pero sobre todo para el análisis y el transporte además de la mejora de presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca por el camino. Si es más fácil acceder a ella también es más fácil modificar su contenido y mucho más pero, desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución.

OBJETIVOS

La información que genere debería de estar en un equipo de cómputo de manera segura, además de actualizar dicha información las veces que sea necesaria o bien que el presidente de la empresa asigne cada fecha de la actualización de los datos o bien de la información, así como una revisión cada año de la información que se va generando día a día en el equipo de cómputo encargado de almacenar la información, también como la eliminación de documentos innecesarios para evitar el almacenaje de información basura o innecesaria para la empresa. Este equipo de cómputo deberá de tener la información de todos los demás equipos de cómputo de toda la empresa para así tener almacenada toda la información en un solo lugar y de esta manera ser más fácil el resguardo y la seguridad de esta información que es valiosa para la empresa.

ORGANIZACIÓN INTERNA

La organización interna tiene como objetivo facilitar la seguridad de la información de cierta empresa u organización para lo cual se debe de tener en cuenta la estructura y controlar la implementación de la seguridad de la información dentro de la organización o empresa.

Asignación de responsabilidades para la seguridad de la información. Como su nombre lo dice se debe de tener un control para definir las responsabilidades que tiene cada persona dentro de la empresa, es decir, que directivo es responsable de cada acción que se realice. Se tienen que documentar los detalles de cada responsable y la responsabilidad de esta.

Sugerencia de tareas. Incluye todo lo relativo a horarios, turnos, tareas. Estos aspectos son importantes ya que de esta manera se les asignan labores a distintas personas con sus diferentes habilidades o discapacidades que pueda tener.

Contacto con las autoridades. Las organizaciones deben de tener procedimientos instalados y que especifiquen cuándo y por qué las autoridades deberían de ser contactadas. Las empresas con un ataque bajo desde el internet pueden necesitar de terceros para tomar acción contra la fuente principal del ataque.

Contacto con los grupos de interés especial. Se deberá de mantener el contacto con las personas responsables de la seguridad que estén especializados para cuando exista algún ataque a la empresa de esta manera se tendrá una mejor comunicación entre las personas especializadas en los ataques informáticos y bajara la probabilidad de robo de información.

Seguridad de la información en la gestión de proyectos. Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación. Por ejemplo los objetivos de control, políticas, procesos y procedimientos de seguridad de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.

DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO

En el uso de la información móvil se debería de considerar los riesgos que implica al momento de trabajar en un dispositivo móvil ya que de esta manera las aplicaciones o bien los entornos están desprotegidos por lo que es conveniente trabajar en una protección más eficiente. La empresa debería de aplicar algunos métodos de protección a lugares remotos y garantizar la seguridad de la información en la movilidad de la información además de establecer una estructura para controlar la implementación de la seguridad de la información dentro de la organización.

Política de uso de dispositivos para movilidad. Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.

Teletrabajo. Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.

FUENTES DE BIBLIOGRAFICAS

- <http://aspectosorganizativosparaseguridad.blogspot.com/>
- <https://docplayer.es/10590019-6-aspectos-organizativos-para-la-seguridad.html>
- <http://seguridatupccc.blogspot.com/2015/05/aspectos-organizativos-para-la.html>
- <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>