Seguridad de la infraestructura de una red

La infraestructura de una red de datos, es la parte más importante de toda nuestra operación como administradores, dado que si nuestra estructura de medio de transporte es débil y no lo conocemos, por lo tanto nuestra red de datos no puede tener un nivel alto de confiabilidad, por lo que en esta sección proporcionaremos las mejores prácticas para tener o mejorar una infraestructura de red confiable.

El avance tecnológico y del conocimiento ha tenido como consecuencia que hoy en día las empresas o negocios se enfrenten a múltiples intrusos o usuarios mal intencionados que intentan vulnerar sus sistemas de información y comunicación. A su vez, internamente, se viven situaciones que podrían afectar la seguridad por descuidos internos, falta de procedimientos, un software mal configurado o decididamente por la falta de políticas de seguridad. Aunado a esto en ocasiones existe la posibilidad de falta de conocimiento por parte del mismo administrador de la red debido a múltiples factores como pueden ser inexperiencia, falta de conocimiento o capacitación. La consecuencia en muchos casos es hacer actividades no planeadas que pueden afectar a la operación diaria de los distintos sistemas. Dado que la información es uno de los activos más importantes de una organización, para cuidarla es necesario administrar sus riesgos con procesos y tecnologías adecuadas y para el administrador de la red defender a la empresa de los múltiples intrusos o problemas internos es una prioridad.

Los desafíos asociados a la seguridad de la información evolucionan muy rápidamente, de forma tal que la tecnología por sí sola no es suficiente y que las políticas de seguridad deben ser acorde con las actividades de su empresa. Gracias a los avances tecnológicos tanto de prevención y corrección de problemas han llevado a los administradores a solicitar o contar con todas las herramientas necesarias para entregar una estrategia fundamentada de seguridad que proteja la totalidad de sus activos de los constantes ataques y vulnerabilidades, cuidando así los tres elementos claves de la seguridad: disponibilidad, integridad y privacidad.

Actualmente existen servicios que permiten cuantificar el nivel de riesgo al que están sujetos los principales activos de información de las empresas, de tal manera que la inversión en seguridad se oriente a análisis de aquellos que afectan principalmente la continuidad y operación diaria del negocio, alcanzando así la mejor relación costo/beneficio. Estos servicios consisten

básicamente en las siguientes etapas: identificación y valoración de activos, vulnerabilidades, amenazas, e identificación de los controles de seguridad ya implementados. Una vez cuantificado el nivel de riesgo, se puede adoptar controles y medidas de seguridad que permitan gestionarlos ya sea reduciendo las amenazas, las vulnerabilidades o bien disminuyendo el impacto frente a algún incidente de seguridad. Como podemos ver el papel de la seguridad es importante y trascendente para garantizar la operación diaria o para controlar los procesos críticos.

PROTECCION DE LA INFORMACION QUE SE TRANSMITE EN UNA RED

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.
Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.
El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

Concepción de la seguridad de la información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:
Crítica: Es indispensable para la operación de la empresa.
Valiosa: Es un activo de la empresa y muy valioso.

Sensible: Debe de ser conocida por las personas autorizadas.

Existen dos palabras muy importantes que son riesgo y seguridad:
Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.**Seguridad**: Es una forma de protección contra los riesgos.