¿Qué entiende por seguridad informática?

La seguridad informatica se encarga de velar por la protecion de la informacion en la organización. Tambien por la integirdad de los equipos de informaticos, identificando y eliminando vulnerabilidades. Cada empresa debe crear politicas de seguridad que se adapten a sus necesidades y exigencias.

¿Cuál considera usted la posible solución o minimización de los riesgos de la seguridad en la red?

Una solucion definitiva es poco probable pero una minimizacion de los riegos si es posible. Considero que el sentido comun debe ser muy aplicado a la seguridad en la red, en nuestras organizaciones debemos implementar habitos que mejoren la seguridad en la red. Debemos estar consientes de los peligros que hay internos y externos, y de las consecuencias que existen cuando somos atacados. Con nuestros datos pueden usurpar identidad y realizar transacciones las cuales nos pueden traer muchos problemas. Es por esto que de la misma forma que se desconfia de un extraño tambien debemos de desconfiar de enlaces, anuncios, promociones y emails.

¿Cuál considera es la mayor amenaza para la seguridad informática en una organización?

La seguridad de informatica ya no es un tema que depende o que solo esta a cargo del area de TI, ya es un responsabilidad de toda la organización. Los riesgos informaticos no solo son externos. Si el enfoque solo esta en proteccion externa cometemos un error. Se debe brindar a los usuarios de buenas practicas de seguridad.

¿Cuál cree usted son los delitos que ocurren con mayor frecuencia en la red interna o externa de la organización?

“Si su organización se está basando en el pasado para proteger su futuro,

su programa de seguridad de la información ya está obsoleto”.

Interesante es aporte tomado del material de estudio, hace que nos esforcemos cada día por innovar en la seguridad informática y con toda razón ya que cada día hay nuevas y mas especializadas formas de burlar los sistemas de seguridad.

**Identificación de riesgos reales**

Para realizar la identificación de riegos reales, se debe examinar donde se encuentra la información mas valiosa y donde se encuentra si afuera o adentro de la organización. También identificar que sistemas están mas expuestos a amenazas o cuales son mas vulnerables.

Amenazas internas: Durante mucho tiempo no se le presto la debida atención a las amenazas internas, y en los últimos años ha venido repuntando como un de los riegos mas relevantes. Las amenazas internas se pueden dar de manera accidental como intencional. Para prevenir las amenazas accidentales se debe orientar al usuario de buenas practicas de seguridad informática. Y para prevenir las amenazas intencionales, aunque un poco mas difícil se puede bajar la probabilidad de que ocurra, esta protección empieza desde la perfilación de los puestos de trabajo y la contratación de personal calificado como también en las restricciones de seguridad y hasta que punto un usuario puede maniobrar información de alta confiabilidad.