La debilidad de una empresa comienza desde el eslabón más débil. El impacto por falta de seguridad informática es muy extenso y poniendo en riesgo, la información privada de una organización hasta el desbanco total de un banco o de una organización. Muchas veces comienza por falta de conocimiento de los usuarios, entrando un virus al almacenamiento del portátil, o dispositivos móviles, de esta forma el virus comienza a desplegarse internamente por la red, por culpa de los empleados, exempleados, colaboradores, proveedores, socios etc. En ocasiones los hacker pueden crear un virus que pueda transportarse en medio de una red, y la meta de ellos es obtener información de los activos con mucho valor.

Todo eso puede traer a la empresa una mala imagen, una reputación baja y una extracción valiosa de información.

De un alto porcentaje la interrupción por una persona o grupo de persona, no autorizadas pueden causar una alta cantidad de perdida en la red, como monetario y de trabajo, debido a los daños o robos de información. De ese método tiene 4 tipos de amenazas los cuales son

* Robo de información
* Robo de identidad
* Perdida y manipulación de datos
* Interrupción del servicio

Estos son los delitos informáticos más frecuentes en la red:

* Abuso del acceso a la red por parte de personas que pertenecen a la organización.
* Virus.
* Suplantación de identidad.
* Uso indebido de la mensajería instantánea.
* Denegación de servicio, caída de servidores.
* Acceso no autorizado a la información.
* Robo de información de los clientes o de los empleados.
* Abuso de la red inalámbrica
* Penetración en el sistema.
* Fraude financiero.
* Detección de contraseñas.
* Registro de claves.
* Alteración de sitios web.
* Uso indebido de una aplicación web publica.

Por eso es importante tener una estrategia buena en prevención de riesgos y amenazas, y unas de las mejores maneras es aplicar las normas de la familia ISO 27000 (27001 y 27002)