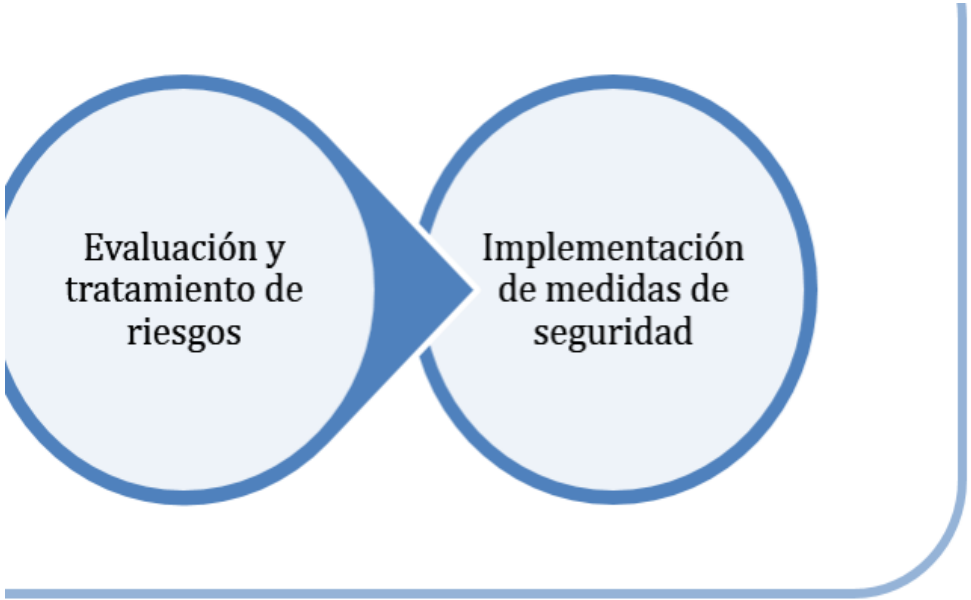
GESTION DE RIESGOS

Normas ISO

Son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos

Se crearon con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de reducir costes y aumentar la efectividad, así como estandarizar las normas de productos y servicios para las organizaciones internacionales.

Gestión del Riesgo



Conceptos

Gestión de Riesgo en la Seguridad Informática: es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Seguridad Informática sirve para la protección de la información, en contra de amenazas, para evitar daños y para minimizar riesgos, relacionados con ella.

Sistema de Gestión de la Seguridad de la Información El SGSI es el concepto sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Datos: es una representación simbólica de una variable cuantitativa o cualitativa.

Información: es toda aquella documentación en poder de una organización e independientemente de la forma en que se guarde o transmita (escrita, representada mediante diagramas o impresa en papel, almacenada electrónicamente, proyectada en imágenes, enviada por fax o correo, o, incluso, transmitida de forma oral en una conversación presencial o telefónica), de su origen (de la propia organización o de fuentes externas) y de la fecha de elaboración.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Así pues, **estos tres términos constituyen la base** sobre la que se cimienta todo el edificio de la seguridad de la información:

Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

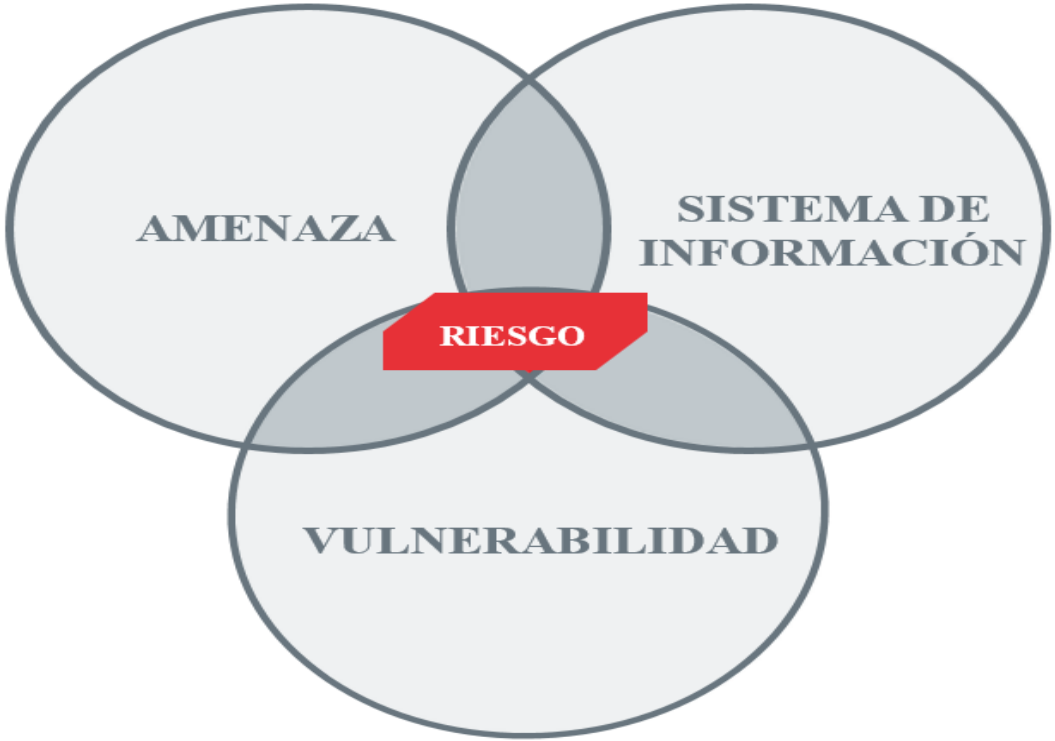
ACTIVO : son los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información.

AMENAZA: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

VULMERALIDAD: es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

SE DENOMINA RIESGO: A LA MEDIDA DEL DAÑO PROBABLE SOBRE UN SISTEMA.


Amenazas
Aprovechan
Vulnerabilidades
Protegen de
Aumentan
Aumentan
Exponen
Controles
Disminuyen
Riesgos
Activos
Imponen
Marcan
Impactan si se materializan
Aumenta
Tienen
Requerimientos de seguridad
Valor de los activos


AMENAZA
SISTEMA DE INFORMACIÓN
RIESGO
VULNERABILIDAD


MIDE EL INTERES DE LOS
Activos
SE MATERIALIZAN SOBRE LOS
Amenazas
SUFREN UNA
Valor
PERMITEN ESTIMAR EL
Degradación
CAUSAN UNA CIERTA
OCURREN CON UNA CIERTA
Impacto
PERMITEN ESTIMAR EL
Frecuencias
Riesgo
LIMITAN EL PERJUICIO
REDUCEN LA OCURRENCIA (Preventivas)
MITIGAN EL
Salvaguardas
LIMITAN EL RIESGO A UN VALOR
Riesgo residual