pirani

Módulo 3

Riesgos, activos y estrategias de seguridad de la información

CONTENIDO

1. Objetivo de la seguridad de la información
2. ¿Qué es una amenaza, un evento y un incidente?
1. Riesgos de seguridad de la información
1. Activos de información e inventario de activos
1. Estrategias de seguridad de la información

1.

Objetivo de la seguridad de la información

Objetivo

El objetivo principal de la seguridad de la información es la **protección de los datos de una organización**, evitar su pérdida y modificación no autorizada.

Confidencialidad

Característica que determina que al activo de información solo puede tener acceso el personal, procesos, sistemas o entidades que están autorizadas.

Integridad

Característica que garantiza la precisión, calidad, veracidad y completitud del activo de información.

Disponibilidad

Característica o cualidad que determina que el activo de información sea oportuno, es decir, que pueda ser consultado y usado por la persona, entidad o proceso autorizados cuando sea requerido.

2.

Amenaza, evento e incidente

Amenaza, evento e incidente

Amenaza

Causa potencial de incidente no deseado, el cual puede resultar en daño al Sistema o a la organización.
Fuente: ISO 27000.

Evento

Presencia identificada de una condición de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas. O una situación desconocida previamente que puede ser pertinente a la seguridad.
Fuente: ISO 27035.

Incidente

Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Fuente: ISO 27035.

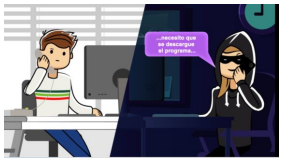
Ejemplos

Amenaza

Vishing

Virus

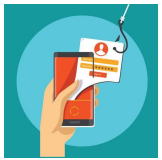
Evento



Llamada

USB infectada

Incidente



Acceso al banco y pérdida de dinero

Computador infectado

3.

Riesgos de seguridad de la información

Amenazas en seguridad a las que está expuesta la organización

Ciclo de los riesgos de seguridad de la información

COMUNICACIÓN

MONITOREO

1. Contexto de SGSI

2. Identificar y valorar los activos

3. Identificación de riesgos SI

4. Evaluación de riesgos

Transferir

Reducir

Evitar

Aceptar

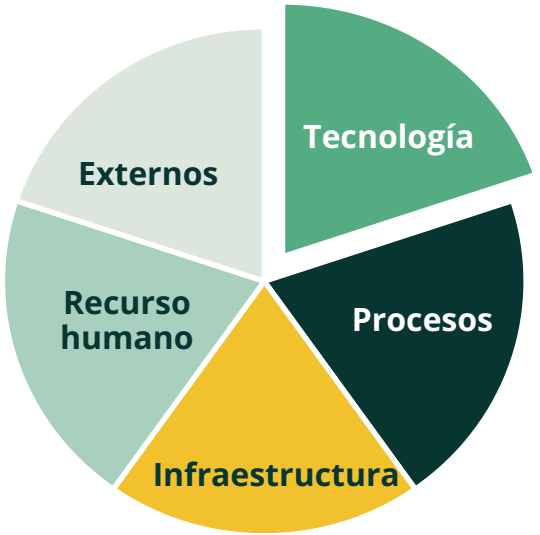
5. Tratamiento

6. Planes de acción

Factores de riesgo a tener en cuenta

Los riesgos de seguridad de la información se deben **identificar con base en la confidencialidad, integridad y disponibilidad de la información** en los activos de información o los procesos, asignando el siguiente orden:

- Número del riesgo
- Descripción
- Activo de información afectado
- Factor de riesgo
- Causas
- Consecuencias
- Calificación



4.

Activos de información e inventario

Tipos de información

Información confidencial

Es aquella cuyo acceso está limitado para los colaboradores y/o terceros con previa autorización por parte del dueño de la información. Lo anterior debido a que su revelación podría causar un impacto operacional, financiero, reputacional y/o legal.

Información restringida

Información de carácter privado o información de uso interno para las áreas o proyectos a la cual se debe tener acceso controlado.

Información de uso interno

Toda información que no sea considerada como confidencial, de conformidad con lo expuesto anteriormente y que es susceptible de ser comunicada a nivel interno de la organización sin restricciones, y solo podrá ser divulgada a un tercero previa autorización del dueño de la información.

Información pública

Es aquella información que puede ser distribuida abiertamente al público sin que cause daño alguno a la organización, a sus colaboradores, otras áreas o sus clientes. Esta categorización solo puede ser asignada por el dueño de la información.

Inventario de activos de información

El inventario y clasificación de los activos de información es la base para la gestión de riesgos de seguridad de la información y para determinar los niveles de protección requeridos. **Se denomina activo a aquello que tiene algún valor para la organización y por lo tanto debe protegerse.**

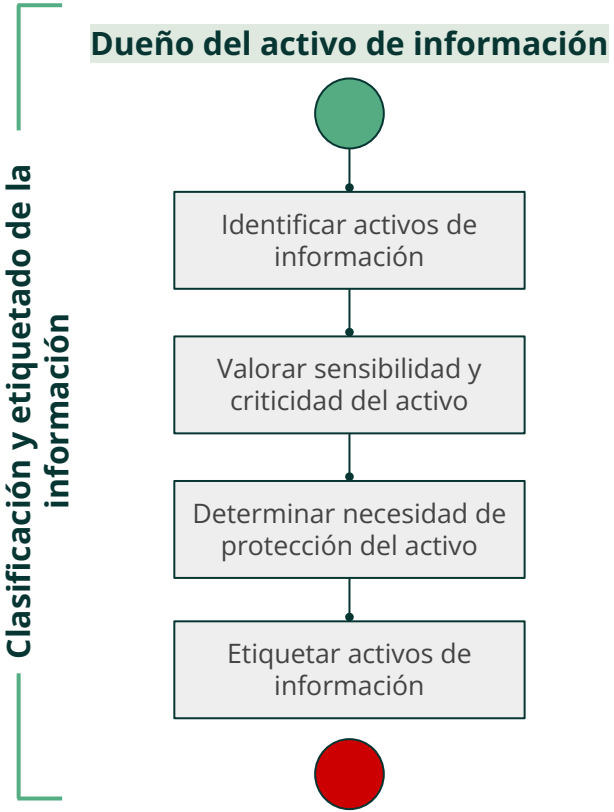
- **Nombre del activo**
- **Descripción**
- **Tipo de activo**
- **Proceso**
- **Propietario**
- **Custodio**
- **Ubicación**

Clasificación
Confidencial
Restringida
Interna
Pública

Valoración de los activos
Leve
Menor
Moderado
Mayor
Grave

Valor del activo y controles
1
2
3
4

Inventario de activos de información



Inventario de activos de información

Valor del activo

Relevancia	Rangos	Criterios	Descripción
Alta	Entre 4 y 5	La confidencialidad, disponibilidad e integridad fueron calificadas en alto.	Uno o varios procesos pueden ser seriamente afectados. Las pérdidas o afectación pueden ser importantes.
Media	Entre 2,5 y 3,9	Los activos que en general en los tres criterios fueron calificados en las escalas medio bajo, medio y medio alto.	El activo puede afectar parcialmente un proceso u operación. Las pérdidas o afectación pueden ser moderadas.
Baja	Entre 1 y 2,4	Los activos que en general obtuvieron calificación baja en los tres criterios.	El activo puede afectar una tarea aislada del proceso u operación. Las pérdidas u afectación serían menores.

5.

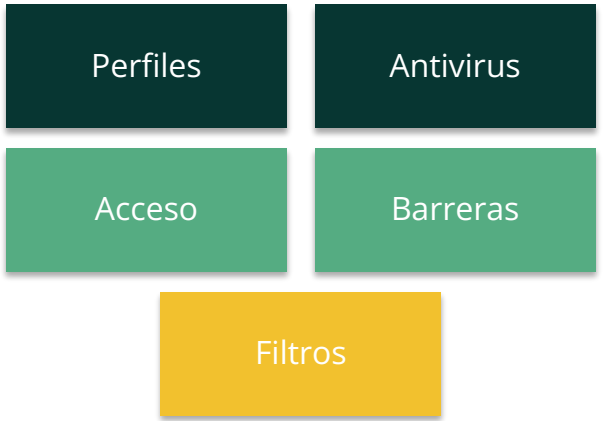
Estrategias de seguridad de la información

¿Cómo definir las estrategias?

Las estrategias de seguridad de la información son resultado de los riesgos e inventario de activos, en el cual **se definen los activos críticos y qué es lo que se va a hacer para proteger los tres pilares de la información que reposa en los activos.**

Como resultado de las estrategias se definen unos procedimientos y controles que se basan en:

- Controles automáticos o manuales
- Políticas
- Guía de seguridad de la información
- Manual de seguridad de la información
- Lineamientos



¡Gracias!

pirani | www.pirani.co/es