

**INSTITUTO POLITÉCNICO NACIONAL**

**ESCOM**

IT GOVERNANCE

3CM10

GUZMAN FLORES JESSIE PAULINA

“ANÁLISIS DE RIESGOS MAQUIMETALICA”

EQUIPO:

Barrios Alvarado Daniel Alejandro

Montaño Europa Sergio

Saldaña Aguilar Gabriela

**ÍNDICE**

1. INTRODUCCIÓN…………………………………………………………………………… 2

1.1 OBJETIVO DE LA EMPRESA…………………………………………………………….... 2

1.2 REQUERIMIENTOS DE LA EMPRESA…………………………………………………… 2

1.3 ACERCA DE LA INFORMACIÓN RECOLECTADA EN LA ENTREVISTA

2. DESARROLLO

2.1 FASE 1 : ANÁLISIS

2.1.1 LISTA DE ACTIVOS Y SU CLASIFICACIÓN

2.1.2 CÁLCULO DEL VALOR DE LOS ACTIVOS

2.2 FASE 2: CLASIFICACIÓN

2.2.1 LISTA DE AMENAZAS

2.2.2 CLASIFICACIÓN DE LAS AMENAZAS

2.2.3 CÁLCULO DEL IMPACTO SOBRE ACTIVO

2.3 FASE 3: REDUCCIÓN

2.3.1 ESCENARIOS Y COSTOS

2.4 FASE 4: CONTROL

2.4.1 PROBLEMAS Y ACCIONES CORRECTIVAS

2.5 GRÁFICAS DE RIESGOS

2.6 SIMULACIÓNES

3. CONCLUSIÓN

**1. INTRODUCCIÓN**

La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su [confidencialidad](https://protejete.wordpress.com/glosario/#confidencialidad), [integridad](https://protejete.wordpress.com/glosario/#integridad) y [disponibilidad](https://protejete.wordpress.com/glosario/#disponibilidad). Considerar aspectos de seguridad significa **a) conocer el peligro, b) clasificarlo y c) protegerse** de los impactos o daños de la mejor manera posible. Esto significa que solamente cuando estamos conscientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos.

El análisis de riesgos como parte del [Sistema de Gestión de Seguridad de la Información](http://blogs.eset-la.com/laboratorio/2011/03/08/principio-pareto-seguridad-informatica/), es necesario para la empresa hacer una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades.

En su forma general contiene cuatro fases

* **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
* **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
* **Reducción**: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
* **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

**1.1 OBJETIVO DE LA EMPRESA**

Ser una solución en maquila de corte làser, punzonado, doblez y soldadura, usando lo màs avanzado entecnologìa CNC para dar a las empresas un mejor servicio.

Poner a su disposición la mejor tecnología en maquinaria de control numérico para doblar, cortar, punzonar y soldar lamina y placa de acero, acero inoxidable, aluminio, etc.

Unirnos a su línea de producción para maximizar su productividad y eficiencia, reduciendo sus tiempos de entrega y aumentando sus ganancias.

**1.2 REQUERIMIENTOS DE LA EMPRESA**

REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES

**RF:**

-Tener una variedad de máquinas y herramientas en la línea de producciòn para los propòsitos establecidos.

-Tener la infraestructura necesaria para tener un ambiente apto para la producciòn.

-Se tendrà un CRM que se encargue de las tareas bàsicas de cada àrea.

-Tener los departamentos en red para una buena coordinaciòn.

-Tener un control de inventario, donde se registren los productos que llegan, los que hay en almacèn y los que se venden.

-Dar capacitaciòn a los usuarios de las màquinas y herramientas.

-El personal debe poder generar las ordenes compra internas y externas dentro del CRM.

-Centralizar y recolectar la información de la empresa para ser procesada y distribuida en los departamentos .

-Cumplir con las mínimas normas de seguridad.

-Invertir en tecnologías de maquinaria CNC de última generación.

-A cada pedido se le deberá asignar un identificador único (id\_pedido), que el usuario podrá copiar al área de almacenamiento permanente de la cuenta.

-Definición de quién puede ingresar datos en el sistema.

-El sistema enviará un correo electrónico cuando se registre alguna de las transacciones.

-Al aprobar un pedido, la solicitud pasará al siguiente paso del flujo de trabajo (workflow) de aprobación configurado en el sistema.

-Al ingresar órdenes de entrega, toda orden de entrega estará asociada a un pedido de venta.

-El proceso de compras en el sistema abarcará los siguientes pasos y transacciones: Ingreso de la requisición, emisión de la solicitud de cotización y emisión de la orden de compra.

-El software debe poder emitir los siguientes estados financieros: Balance general, Estado de ganancias y pérdidas, Estado de flujos de efectivo. Además, debe poder emitir un listado de mayor general y mayor analítico.

-Los campos que comprenden la mayoría de las operaciones son: numéricos o alfanuméricos, dependerá de lo solicitado.

-Cualquier pantalla de pago puede imprimir los datos en la impresora.

-Los integrantes del grupo de usuarios de gerentes pueden ingresar y aprobar solicitudes, pero no pueden borrarlas.

-Los integrantes del grupo de usuario de administradores no pueden ingresar o aprobar solicitudes, pero si pueden borrarlas.

-El software podrá ser utilizado en los sistemas operativos Windows, Linux y OSX.

**RNF:**

**-**Se deberá hacer un respaldo de la información de forma semanal.

-Las iterfàces deberán usar el estilo de diseño establecido por los directores, ya que aseguran que es màs sencillo de usar si todo tiene una homogeneidad.

-Monitorear y checar los horarios de entrada y salida de cada uno de los trabajadores.

-Entregar puntualmente, resultado de la eficiencia y redundancia en máquinas.

-Toda funcionalidad del sistema y transacción de negocio debe responder al usuario en menos de 10 segundos.

-Los datos modificados en la base de datos deben ser actualizados para todos los usuarios que acceden.

-Los permisos de acceso al sistema podrán ser cambiados solamente por el administrador de acceso a datos.

-El sistema no continuara operando en caso de fuego.

-El tiempo de aprendizaje del sistema por un usuario deberá ser menor a 4 horas.

-El sistema debe proporcionar mensajes de error que sean informativos y orientados a usuario final.

-El sistema debe poseer interfaces gráficas bien formadas.

-El sistema debe tener una disponibilidad del 99,99% de las veces en que un usuario intente acceder.

-Debe haber suficiente memoria RAM para el CRM.

-El proceso de desarrollo se gestionará por medio de una determinada herramienta.

-Debe especificarse un plan de recuperación ante desastres para el sistema a ser desarrollado.

**1.3 ACERCA DE LA INFORMACIÓN RECOLECTADA EN LA ENTREVISTA**

----------------------------------- A CERCA DE LA EMPRESA -------------------------

\*Página web: http://www.maquimetalica.com/

\*Empresa de maquilación que ofrece corte láser, punzonadoras de torreta, soldadura y doblez.Cuenta con lo más avanzado en tecnología CNC.

\*Cuenta con los siguientes departamentos: Ventas,Posventa o Servicios, Recursos humanos, IT, Administración y Contabilidad, Marketing, Intendencia,Producción, Atencion a clientes

\*Materiales que manejan: Acero , aluminio, acero inoxidable, etc…

\*Para corte por láser se tienen las siguientes tecnologías:

1-CNC de Alta Velocidad por Fibra Óptica con Láser 2KW IPG

2-Cortadora Láser CNC de 5´x 10´x 4000 Wts

3-Cortadora Láser CNC de 5´x 10´x 2500 Wts

\*Para punzonado se tiene las siguientes tecnologías:

1-Punzonadora de Torreta CNC de 4´x 8´x 25 Tons.

2-Punzonadora de Torreta CNC de 4´x 4´x 30 Tons.

\*Solo hay cursos de capacitación para el personal que se dedica a usar las máquinas y herramientas

\*Para la dobladora de làmina se tiene:

1-Dobladora CNC de 10´de largo y 120 Tons

2-Dobladora CNC de 12´ de largo y 250 Tons

\*Soldadura:

1-Soldadoras MIG Programables

2-Robot Soldador por MIG

\*Que datos del cliente son los que se guardan

---------------------------------- A CERCA DE LAS NORMATIVIDADES -------------------------

\*Falta implementar normas

\*Cumplen con las mínimas de seguridad

\*Falta certificar la red, por ahora es categoría 5E cuando debería ser 6E

----------------------------------------- A CERCA DE LA INFRAESTRUCTURA -------------------------

\*Ampliar área de IT, es sólo un cuarto dedicado al encargado de IT.

\*La empresa tiene una arquitectura distribuida, tiene 3 servidores: Uno en el estado de México que se encarga de la administración del catálogo de clientes, catálogo de artículos, facturación, recursos humanos, órdenes internas, cotización, control de material siendo utilizado en el momento, otro en Querétaro y otro en Illinois EUA.

\*El servidor principal que se encuentra en Edo.Mex contiene el sistema CRM, el servidor principal de Querétaro contiene una parte del CRM, el servidor de Illinois es un servidor de correo electrónico y ERP.

\*El CRM está dividido en dos partes la parte virtualizada y la parte nativa o local que se usa para la programación numérica de las máquinas y herramientas.

\*Las máquinas y herramientas de corte, doblado y punzonado no están en red, pero es posible ponerlas en red para mandarles los programas que necesitan para generar el producto de forma automática.

\*Los relojes checadores están en red y el CRM contabiliza los retardos

\*Infraestructura de red marca epcom: 1 switch de 10/100, 1 patch, 1 grabador DVR para 16 cámaras funcionando 24/7 365º, 1 ups, 1 servidor MAC pro

\*Se tiene un enlace E1 para la red industrial y áreas locales de 50 Mb de banda de ancho como puntos de acceso a internet, Telmex.

--------------------------------- A CERCA DEL PERSONAL -------------------------

\*El encargado del área de IT tiene a cargo los siguientes trabajos: Servicios,Seguridad,Mantenimiento,Inventarios,Desarrollo, Comunicaciones,Sistemas

----------------------------------------- A CERCA DEL HARDWARE -------------------------

\*Los servidores cuentan con el mínimo de los requerimientos de capacidad en memoria, velocidad de procesamiento y software necesario.

\*El servidor CRM cuenta con las siguientes especificaciones: 32 GRAM, 350 GB disco duro de estado sólido, este tiene un dongleUSB que cuenta con los permisos necesarios para poder usar la programación de control numérico, costo aproximado de $60,000 (Apple Mac Pro MD878E/A, Intel Xeon E5-1650V2 3.50GHz, 16GB (4 x 4 GB), 256GB, Mac OS X 10.9 Mavericks 64-bits)

----------------------------------------- A CERCA DEL SOFTWARE ------------------------

\*El servidor principal contiene un sistema CRM el cual tiene los siguientes roles: administrador y general, se dan permisos especiales para cada departamento ( lista de deptos ).

\*Todo el equipo de cómputo tiene Sftw con licencia y es original, la licencia se renueva anualmente.

\*El CRM es el encargado de centralizar los datos y formatos para tener una homogeneidad en la empresa, realiza transacciones bàsicas (CRUD), lleva el control de inventario, planeación de recursos, asignación de tareas mediante un calendario virtual, control de acceso de personal (chequeo electrónico), graficas de gantt, genera la factura en pdf y xml, y se piensa escalar a un SAE aspel.

\*Las herramientas que el CRM contiene han sido programadas en el establecimiento.

\*En el desarrollo del CRM usan un ambiente de desarrollo àgil llamado Filemaker.

\*No existe interfaz para el cliente donde pueda cotizar y facturar su pedido.

\*No existe una uniformidad en marcas ni Sftw, hay desde

-Windows XP, Server,10

-MAC pro,tiger, leopard,lion

-Linux Ubuntu

\*El control de inventario se realiza con Filemaker

\*El CRM debe poder emitir los siguientes estados financieros: Balance general, Estado de ganancias y pérdidas, Estado de flujos de efectivo. Además, debe poder emitir un listado de mayor general y mayor analítico.

----------------------------------------- A CERCA DE LA SEGURIDAD -------------------------

\*Invertir en Firewalls, para cifrar datos

\*No se tiene un dominio como tal, se usa un active directory

\*El servidor principal no tiene un espacio para sí solo, tiene dos formas para acceso: nivel aplicación y hardcore

\*Se realiza un respaldo de la información semanal y de forma manual, se tiene una copia de esta información en otro ordenador externo al servidor.

\*Los distintos departamentos involucrados en la empresa si están comunicados, no existe una VPN, los permisos para poder utilizar los puertos se hacen de forma manual, falta mejorar la seguridad.

\*El servidor CRM no cuenta con algún tipo de seguridad física,como aislamiento, enfriamiento, etc..

----------------------------------- A CERCA DE LA DOCUMENTACIÓN -------------------------

\*No existe una documentación formal de lo que se ha desarrollado en el àrea de IT, ni manual de procedimientos en caso de contingencias.

\*Los documentos administrativos y de compraventa no están respaldados 100%, solo una parte

---------------------------- A CERCA DEL MANUAL DE OPERACIONES -------------------------

\*Se tiene soporte tècnico en caso de que algún dispositivo falle.

\*No existe un manual de operaciones específico.

**NOTAS:**

**Enlace dedicado E1:** Es un enlace que consta de 32 canales de 64 kbps cada uno 31 son usados para la transmisión de datos y uno para la señalización esto es la norma europea,este enlace puede ir conectado a una nube de MPLS de algún proveedor de servicios,así puedes enlazar sucursales remotas y poder transmitir voz y datos por este enlace el cual es totalmente privado.

**CNC**:El control numérico por computadora, de ahora en adelante CNC, es un sistema que permite controlar en todo momento la posición de un elemento físico, normalmente una herramienta que está montada en una máquina. Esto quiere decir que mediante un software y un conjunto de órdenes, controlaremos las coordenadas de posición de un punto (la herramienta) respecto a un origen (0,0,0 de máquina), o sea, una especie de GPS pero aplicado a la mecanización, y muchísimo más preciso. No solo controla las coordenadas que hemos visto, sino también, la manera de desplazarse entre ellas, su velocidad, y algunos parámetros más. Un CNC es un equipo totalmente integrado dentro de máquinas-herramienta de todo tipo, de mecanizado, de corte, por láser, cortadoras, etc.

**SAE aspel:** Aspel-SAE 6.0 es el Sistema Administrativo Empresarial más vendido en México y el único que pone en control total a tu negocio.

Controla el ciclo de todas las operaciones de compra-venta de la empresa, como inventarios, clientes, facturación, cuentas por cobrar, vendedores, compras, proveedores y cuentas por pagar, automatizando eficientemente los procesos administrativos. Ofrece movilidad a las empresas conectando las sucursales remotamente y por medio de dispositivos móviles; permite el acceso a la información comercial y administrativa, brindando una integración total. Poderosa interfaz con Aspel-COI para relacionar los folios fiscales de los Comprobantes Fiscales Digitales a las pólizas, de acuerdo con los requerimientos de la Contabilidad Electrónica.

**CRM (customer relationship management):**Software para la administración de la relación con los clientes. Sistemas informáticos de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing. [2](https://es.wikipedia.org/wiki/Customer_relationship_management#cite_note-2) Dicho software puede comprender varias funcionalidades para gestionar las ventas y los clientes de la empresa: automatización y promoción de ventas, tecnologías [data warehouse](https://es.wikipedia.org/wiki/Data_warehouse) (almacén de datos) para agregar la información transaccional y proporcionar capa de reporting, dashboards e indicadores claves de negocio, funcionalidades para seguimiento de campañas de marketing y gestión de oportunidades de negocio, capacidades predictivas y de proyección de ventas.

**Dongle USB:**ofrecen la posibilidad de llevar a cabo transferencias rápidas de datos entre dos computadoras, como así también permite compartir la conexión de red sin necesidad de requerir de drivers, permiten añadir características a las [computadoras](http://www.informatica-hoy.com.ar/hardware-pc-desktop/Que-es-una-computadora.php) que no fueron construidas teniendo en cuenta dichos parámetros.

**Punzonadora:** Una punzonadora es un tipo de máquina que se usa para perforar y conformar planchas de diferentes materiales usando un [punzón](https://es.wikipedia.org/wiki/Punz%C3%B3n) y una matriz a semejanza de una prensa.

**FileMaker:**FileMaker Pro es un potente software que permite crear apps personalizadas que funcionan perfectamente en iPad, iPhone, Windows, Mac y la Web.

Cree fácilmente su propia app personalizada para satisfacer las necesidades exclusivas y en constante cambio de su negocio. O bien inspírese con las Soluciones Iniciales integradas para la gestión de contactos, inventarios, contenidos, y más.

**2. DESARROLLO**

Como antes se mencionó dividiremos el trabajo en 4 etapas que describiremos a continuación.

**2.1 FASE 1 : ANÁLISIS**

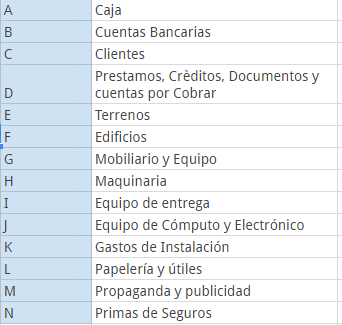
Se realizarán las siguientes actividades:

-Catálogo de riesgos

-Identificar los activos de la empresa

-Clasificar qué tan valioso es el activo **VA** ya sea para la propia empresa o para la competencia, quienes son los involucrados **.**

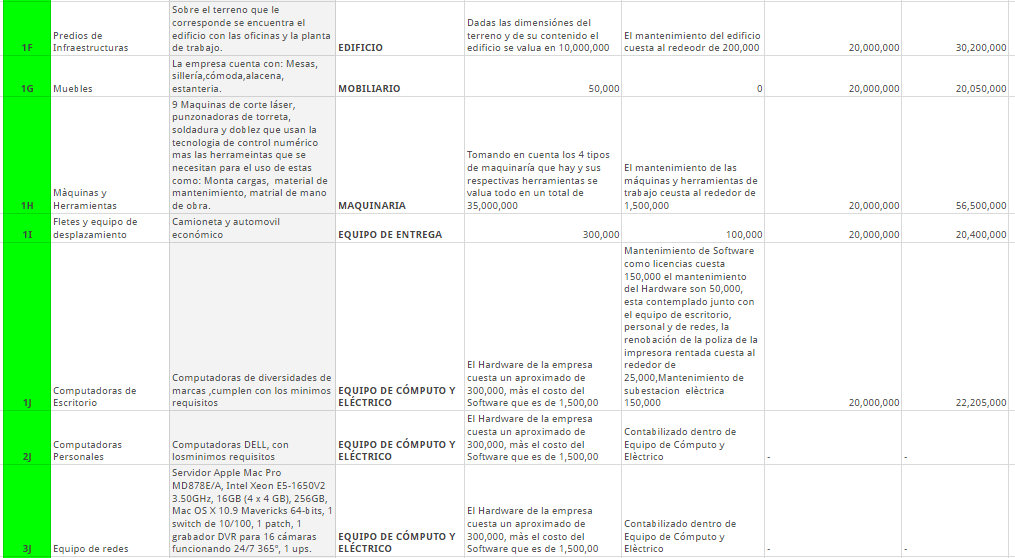
**2.1.1 LISTA DE ACTIVOS Y SU CLASIFICACIÓN**

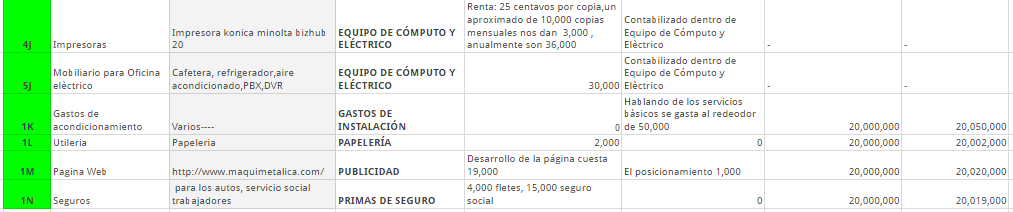


****

**2.1.2 CÁLCULO DEL VALOR DE LOS ACTIVOS**

****

****

****

****

**2.1.3 CATÁLOGO DE RIESGOS**

****

**2.2 FASE 2: CLASIFICACIÓN**

Se realizarán las siguientes actividades:

-Identificar que tipo de riesgo es : Amenaza, Vulnerabilidad, Superposición.

-Identificar que tipo de amenaza es: Repercutido, Residual, Acumumlado.

## Impacto acumulado

Puesto que los activos dependen unos de otros, la materialización de amenazas en los activos inferiores causa un daño directo sobre éstos y un daño indirecto sobre los activos superiores.

El impacto acumulado es el impacto evaluado en los activos inferiores.

El impacto acumulado se calcula tomando en cuenta;

* el valor acumulado y
* la degradación causada por la amenaza

impacto\_acumulado = valor\_acumulado \* degradación

Los activos se relacionan unos con otros, de forma que el efecto de una amenaza en un activo tiene consecuencias indirectas en los activos que dependen del activo directamente dañado.

Impacto repercutido

Mide el daño en los activos superiores.

El impacto repercutido se calcula tomando en cuenta:

* el valor propio del activo superior
* la degradación causada por la amenaza en el activo inferior
* el grado de dependencia del activo superior del activo inferior

Básicamente, la degradación del activo inferior repercute sobre el activo superior en la medida indicada por el grado de dependencia:

impacto repercutido = valor \* degradación \* grado

## Impacto residual

Las salvaguardas reducen la degradación causada por una amenaza en un activo.

Si evaluamos el impacto tomando en consideración el efecto mitigador de las salvaguardas, el nuevo valor del impacto se llama residual.

-Identificar qué tan tan expuestos están esos activos a las amenazas existentes por activo **FE.**

## Identificación del factor de exposición

El factor de exposición es el porcentaje de pérdida potencial para un activo, si una amenaza específica se materializa. Es un elemento subjetivo, que debe ser definido por el encargado de realizar el cálculo; sin embargo, a pesar de la subjetividad, debe utilizar criterios consistentes, para obtener resultados repetibles. Por ejemplo:

-Identificar la tasa de ocurrencia anual de vulnerabilidad por activo. Cada cuanto está en riesgo el activo en un periodo de un año **TOA.** Para calcular el **TOA** primero obtuvimos el equivalente del porcentaje de incidencias por riesgo a días del año, después agrupamos que riesgos afectan a qué activos y sacamos el promedio de esos riesgos.

Tasa de Incidencia

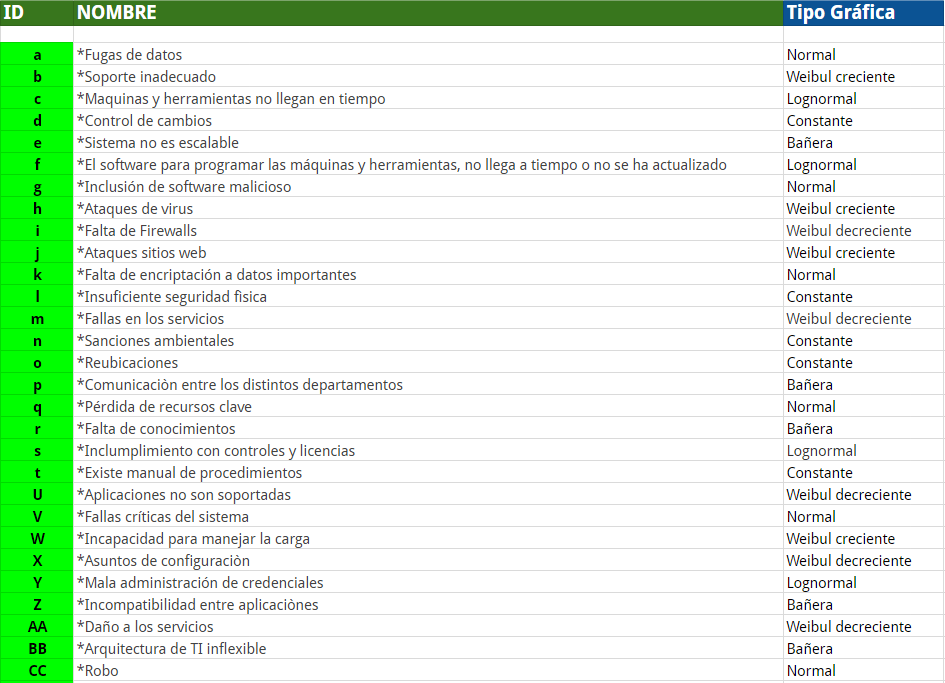
Se define como el número de nuevos casos que se producen durante un periodo especificado en una población en riesgo.Se debe fijar el período de observación de ocurrencia del EVENTO a medir por un período específico de TIEMPO.

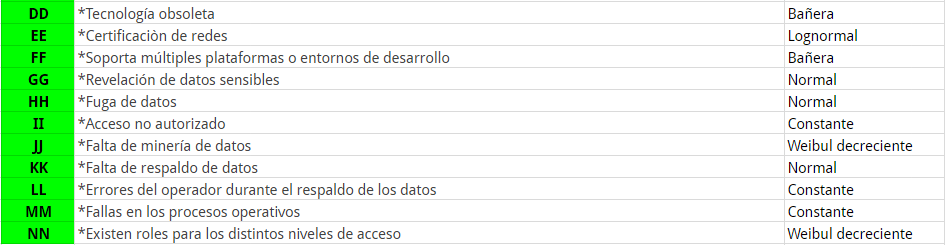
-Determinar la expectativa de pérdida simple **EPS** que es la multiplicación de **VA\*FE** por activo.

-Determinar la expectativa de pérdida anual **EPA = TOA\*EPS**

-Priorizar activos por **EPA, enlistarlos del mayor al menor**

**2.2.1 LISTA DE AMENAZAS**

****

****

**2.2.2 CLASIFICACIÓN DE LAS AMENAZAS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Nombre** | **Amenaza** | **Vulnerabilidad** | **Suposición** | **Ocurrencia** | **Descripción** | **Responsables / afectados** |
| a | Fuga de datos | X | X |  | 80% (.70) | Existe la posibilidad de que exista una fuga de datos de nuestros clientes y proveedores | El responsable sería el encargado de sistemas ya que el acceso al sistema es vulnerable y los afectados seria la empresa |
| b | Soporte inadecuado |  | X |  | 40% (.45) | Aquí hace referencia que puede que no se le dé el seguimiento adecuado a las ordenes porque el sistema no es eficiente | El área de ventas ya que se puede perder ventas por el mal funcionamiento |
| c | Máquinas y herramientas no llegan a tiempo |  |  | X | 20% (.15) | Puede llegar a ocurrir que la persona encargada de ingresar los pedidos de máquinas o herramientas nuevas no las ingrese a tiempo o que el sistema sufra un fallo | El área de producción seria el afectado por lo mismo de que llegan tarde las máquinas, piezas u otras cosas se atrasan las ordenes |
| d | Control de cambios |  | X |  | 65% (.70) | Cuando se necesita cambiar algún programa o actualizarlo y no se le informa al personal puede que se genere un mal uso de este | El responsable es el encargado de sistemas ya que debe de informar de los cambios y explicar si es que existe algún procedimiento diferente |
| f | El software para programar las máquinas y herramientas, no llega a tiempo o no se ha actualizado |  | X |  | 50% (.45) | Si no está el programa o esta desactualizado la producción no será eficiente y atrasara las ordenes ya hechas | El responsable es el del área de sistemas y el afectado principal seria el área de producción |
| g | Inclusión de software malicioso | X |  |  | 85% (.90) | Si por alguna razón un empleado ingresa o instala un software que no sepa de donde proviene o quien es el desarrollador puede hacer que el equipo no funcione de manera correcta | El del área de sistemas |
| h | Ataque de virus | X |  |  | 90% (.90) | Puede que por páginas, programas o dispositivos usb las maquinas tenga virus | El área de sistemas porque debe revisar que el antivirus esté funcionando de manera adecuada |
| i | Falta de firewalls |  |  |  |  |  |  |
| j | Ataques al sitio web | X |  |  | 35% (.45) | El sitio web puede sufrir ataques y si se cae nuestros clientes no tendrán información de acerca de nosotros | El de sistemas debe cuidar que el sitio este arriba siempre y exista un respaldo de la información |
| k | Falta de encriptación a información importante | X |  |  | 85% (.90) | Si la información de valor no está encriptada cualquier persona podría tener acceso a ellos | Todos los que manejen esa información deberían encríptalos para así hacer más seguro el manejo de la misma |
| l | Suficiente seguridad física |  | X |  | 90% (.90) | Se debe cuidar también de manera física quien tiene acceso a la información | El encargado de sistemas |
| m | Fallas en los servicios |  | X |  | 90% (.90) | Que cualquier servicio o recurso físico falle o se descomponga | El área de sistemas le debe dar el mantenimiento adecuado |
| n | Sanciones ambientales |  |  | X | 20% (.15) | Se pueden tener sanciones ambientales por desechar de manera inadecuada materiales electrónicos o residuos peligrosos | El afectado seria la empresa, ya que la multa tendría que ser pagada por la empresa |
| o | Reubicaciones |  |  | X | 20% (.15) | Se debe avisar si existen reubicaciones de máquinas o equipos para hacer más fácil el trabajo |  |
| p | Comunicación entre los distintos departamentos |  | X |  | 80% (.70) | Es importante que todas la reas estén conectada para que los procesos se lleven de manera adecuada y no exista perdida de información | Si no existe la comunicación todas las áreas resultan afectadas |
| q | Pérdida de recursos claves | X |  |  | 90% (.90) | Si se pierden recursos claves, del personal existe la posibilidad de que el trabajo no se realice de manera optima | Todos los empleados y responsables de área deben cuidar y estar pendiente de los recursos y llevar un control de inventarios |
| r | Falta de conocimientos |  | X |  | 80% (.70) | Cuando el personal no está adecuadamente capacitados o no tiene los conocimientos necesarios para manejar algún programa o maquina existe un trabajo deficiente | En lo que respecta con los conocimientos programas y maquina el responsable del área de sistemas debe dar una pequeña capacitación a los empleados para que no hay problemas |
| s | Incumplimientos de controles y licencias | X |  |  | 90% (.90) | En caso de no contar con controles de calidad o licencias se puede perder información y ser acreedores a una multa | El responsable del área de sistemas debe checar que todo esté en orden, porque en caso contrario la empresa será acreedora de una multa |
| t | Existe manual de procedimientos |  | X |  | 40% (.45) | Es importante que exista el manual de procedimientos y que se haga lo que establece para evitar problemas |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Nombre** | **Descripción** | **A** | **V** | **S** | **Ocurrencia** | **Responsables / Afectados** |
| U | Aplicaciones no son soportadas | La aplicación no es soportada ya sea por compatibilidad o requisitos mínimos |  |  | X | 35% (.45) | Afectado: La sección en la que la aplicación valla a funcionar  Responsable: El encargado de analizar los requisitos mínimos del sistema |
| V | Fallas críticas del sistema | Se producen errores que afectan el funcionamiento del sistema. | X |  |  | 10% (.15) | Afectado: La sección en la que el sistema valla a funcionar  Responsable: El encargado de darle mantenimiento al sistema |
| W | Incapacidad para manejar la carga | No cuenta con la infraestructura necesaria para poder manejar la carga de datos | X |  |  | 35% (.40) | Afectado: La parte administrativa de la empresa  Responsable: El DBA |
| X | Asuntos de configuración | El sistema no fue configurado total o parcialmente |  | X |  | 20% (.15) | Afectado: Todo el personal que valla a interactuar con el sistema  Responsable: El encargado de darle mantenimiento al sistema |
| Y | Mala administración de credenciales | Permite el acceso a los distintos niveles a cualquier personal activo |  | X |  | 40% (.45) | Afectado: Todo el sistema en general, debido a la falta de control  Responsable: El encargado del sistema para las secciones del mismo y el DBA para los accesos en la base de datos |
| Z | Incompatibilidad entre aplicaciones | Las aplicaciones no pueden intercambiar información entre ellas |  |  | X | 35% (.40) | Afectado: Los módulos que no puedan interactuar entre si  Responsable: El encargado de analizar los requisitos mínimos del sistema |
| AA | Daño a los servicios | Daños ocasionados por terceras personas al sistema (hackers) | X |  |  | 10% (.15) | Afectado: El sistema en general debido a la vulnerabilidad y posible pérdida de información.  Responsable: El encargado de la seguridad del sistema |
| BB | Arquitectura de TI inflexible | No permite o tolera cambios a las practicas que ya definió |  | X |  | 50% (.45) | Afectado: El personal en general debido a la resistencia a cambios  Responsable: Gobierno de TI |
| CC | Robo | Robo total o parcial a los equipos de cómputo o maquinaria en general | X |  |  | 35% (.45) | Afectado: La empresa en general  Responsable: La seguridad con la que cuente la empresa |
| DD | Tecnología obsoleta | Falta de recursos para implantar un sistema actualizado |  | X |  | 66% (.70) | Afectado: El sistema debido a que no podrá instalarse o correr óptimamente.  Responsable: El encargado de analizar los requisitos mínimos del sistema |
| EE | Certificación de redes | Se comprueba que la instalación de esa red cumple los parámetros técnicos necesarios para cumplir con la normativa internacional relacionada con el tipo de instalación. |  |  | X | 30% (.15) | Afectado: Interacción entre módulos del sistema (Sistema en general)  Responsable: El encargado de instalar y dar mantenimiento a las Redes |
| FF | No soporta múltiples plataformas o entornos de desarrollo | No permite la interacción de sistemas desarrollados en diferentes plataformas |  |  | X | 15% (.15) | Afectado: El sistema en general debido a la falta de comunicación entre módulos  Responsable: El encargado de analizar los requisitos mínimos del sistema |
| GG | Revelación de datos sensibles | Expone información personal sobre clientes y proveedores así como datos privados de la compañía | X |  |  | 66% (.70) | Afectado: Toda la empresa, ya que podríamos perder datos que nos produzcan perdidas económicas, como la cartera de clientes  Responsable: El encargado de la seguridad del sistema |
| HH | Fuga de datos | La información de nuestros clientes y proveedores puede ser robada. | X |  |  | 80% (.70) | Afectado: Toda la empresa, ya que podríamos perder datos que nos produzcan perdidas económicas, como la cartera de clientes  Responsable: El encargado de la seguridad del sistema o el DBA a la base de datos |
| II | Acceso no autorizado | Personal no autorizado o ajeno a la compañía acceda a nuestra base de datos |  | X |  | 80% (.70) | Afectado: La empresa en general debido a la posible pérdida o robo de datos.  Responsable: El encargado de la seguridad del sistema o el DBA a la base de datos |
| JJ | Falta de minería de datos | No se pueden extraer datos precisos o analizar grandes volúmenes de datos |  | X |  | 65% (.45) | Afectado: La área productiva de la empresa por la falta de datos para tomar decisiones importantes  Responsable: El encargado de analizar la base de datos |
| KK | Falta de respaldo de datos | No se realizan respaldos preventivos lo que puede ocasionar pérdida total de información |  | X |  | 80% (.70) | Afectado: La empresa y sistema en general por la posible pérdida de datos importantes  Responsable: El DBA |
| LL | Errores del operador durante el respaldo de los datos | El encargado comete un error al respaldar provocando daño o perdida de información |  |  | X | 50% (.45) | Afectado: La empresa y sistema en general por la posible pérdida de datos importantes  Responsable: El DBA por la falta de supervisión y el encargado por la falta de experiencia |
| MM | Fallas en los procesos operativos | No se cumplen los requisitos de los clientes |  | X |  | 50% (.45) | Afectado: La empresa debido a la inconformidad que presentaran los clientes  Responsable: El encargado de supervisar y monitorear las peticiones de los clientes |
| NN | No existen roles para los distintos niveles de acceso | Permite el acceso a los distintos niveles a cualquier personal activo |  | X |  | 50% (.45) | Afectado: La empresa en general debido a la posible pérdida o robo de datos.  Responsable: El encargado de la seguridad del sistema o el DBA a la base de datos |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Tipo** | **Residual** | **Acumulado** | **Repercutido** | **ID activos impactados** |
| a | Amenaza | X |  |  | 1A, 2A, 1B, 1C, 1D, 2D, 3D |
| b | Vulnerabilidad | X |  |  | 1H, 1I, 1J |
| c | Suposición | X |  |  | 1H, 1I, 1J |
| d | Vulnerabilidad |  | X |  | 1J, 2J, 3J, 4J, 5J |
| f | Vulnerabilidad |  | X |  | 1H, 1J, 2J, 3J, 4J, 5J |
| g | Amenaza |  |  | X | 1H, 1J, 2J, 3J, 4J, 5J |
| h | Amenaza |  |  | X | 1H, 1J, 2J, 3J, 4J, 5J |
| i | Amenaza |  | X |  | 1H, 1J, 2J, 3J, 4J, 5J |
| j | Amenaza |  | X |  | 1H, 1J, 2J, 3J, 4J, 5J |
| k | Amenaza |  | X |  | 1B, 1C, 1D, 2D, 1E, 1F, 1G, 1M |
| l | Vulnerabilidad |  |  | X | 1A, 2A, 1B, 1G, 1H, 1J, 2J, 3J, 4J, 5J |
| m | Vulnerabilidad |  |  | X | 1A, 2A, 1H, 1J, 2J, 3J, 4J, 5J |
| n | Suposición | X |  |  | 1G, 1H, 1M |
| o | Suposición | X |  |  | 1G, 1H, 1J, 2J, 3J, 4J, 5J |
| p | Vulnerabilidad | X |  |  | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1E, 1F |
| q | Amenaza |  |  | X | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1E, 1F |
| r | Vulnerabilidad | X |  |  | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1E, 1F, 1G, 1H, 1J, 2J, 3J, 4J, 5J, 1M, 1N |
| s | Amenaza |  |  | X | 1J, 2J, 3J, 1M |
| t | Vulnerabilidad | X |  |  | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1E, 1F, 1G, 1H, 1J, 2J, 3J, 4J, 5J, 1M, 1N |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Tipo** | **Residual** | **Acumulado** | **Repercutido** | **ID’s de Activos impactados** |
| U | Suposición | x |  |  | 1K, 1M |
| V | Amenaza | x |  |  | 1B, 1C, 3D, 1H,1J, 2J, 3J, 4J, 5J, 1M |
| W | Amenaza |  | x |  | 1B, 1C, 1D, 3D, 1I, 1M |
| X | Vulnerabilidad |  | x |  | 1B, 1C, 1D, 3D, 1I, 1M |
| Y | Vulnerabilidad | x |  |  | 1A, 2A, 1B, 1C, 3D, 1J, 2J |
| Z | Suposición | x |  |  | 1J, 2J, 3J, 4J, 5J |
| AA | Amenaza |  |  | x | 1M |
| BB | Vulnerabilidad |  |  | x | 1J, 2J, 3J, 1M |
| CC | Amenaza |  | x |  | 1A, 2A, 1G, 1I, 1J, 2J, 3J, 4J, 5J, 1L |
| DD | Vulnerabilidad |  | x |  | 1H, 1J, 2J, 3J, 4J, 5J, 1M |
| EE | Suposición |  | x |  | 1J, 2J, 3J, 4J. 5J |
| FF | Suposición | x |  |  | 1B, 1J, 2J, 3J, 4J |
| GG | Amenaza | x |  |  | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1J, 2J |
| HH | Amenaza | x |  |  | 1A, 2A, 1B, 1C, 3D, 1J, 2J |
| II | Vulnerabilidad | x |  |  | 1A, 2A, 1B, 1C, 3D, 1J, 2J |
| JJ | Vulnerabilidad | x |  |  | 1B, 1M |
| KK | Vulnerabilidad |  |  | x | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1J, 2J |
| LL | Suposición |  |  | x | 1A, 2A, 1B, 1C, 1D, 2D, 3D, 1J, 2J |
| MM | Vulnerabilidad |  | x |  | 1A, 2A, 1B, 1C |
| NN | Vulnerabilidad |  | x |  | 1A, 2A, 1B, 1C, 3D, 1J, 2J |

**2.2.3 CÁLCULO DEL IMPACTO SOBRE ACTIVO**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID Activo** | **ID’s Riesgos** | **FE** | **TOA** | **EPS (VA\*FE)** | **EPA (TOA\*EPS)** |
| 1A | a, l, m, p, q, r, t, Y, CC, GG, HH, II, KK, LL, MM, NN | 30% | [(80\*365/100) + (90\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) + (35\*365/100) + (35\*365/100) + (66\*365/100) + (35\*365/100) + (80\*365/100) + (80\*365/100) + (50\*365/100) + (50\*365/100) + (50\*365/100)] / 16 = 235 | 20,005,000\*.30 = 6,001,500 | 1,410,352,500 |
| 2A | a, l, m, p, q, r, t, Y, CC, GG, HH, II, KK, LL, MM, NN | 45% | [(80\*365/100) + (90\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) +(35\*365/100) + (35\*365/100) + (66\*365/100) + (35\*365/100) + (80\*365/100) + (80\*365/100) + (50\*365/100) + (50\*365/100) + (50\*365/100)] / 16 = 235 | - | - |
| 1B | a, k, l, p, q, r, t, V, W, X, Y, FF, GG, HH, II, JJ, KK, LL, MM, NN | 25% | [(80\*365/100) + (85\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) + (10\*365/100) + (35\*365/100) + (20\*365/100) + (40\*365/100) + (15\*365/100) + (66\*365/100) + (80\*365/100) + (80\*365/100) + (65\*365/100) + (80\*365/100) + (50\*365/100) + (50\*365/100) + (50\*365/100)] / 20 = 216 | 21,500,000\*.25 = 5,375,000 | 1,161,000,000 |
| 1C | a, k, p, q, r, t, V, W, X, Y, FF, GG, HH, II, JJ, KK, LL, MM, NN | 25% | [(80\*365/100) + (85\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) + (10\*365/100) + (35\*365/100) + (20\*365/100) + (40\*365/100) + (15\*365/100) + (66\*365/100) + (80\*365/100) + (80\*365/100) + (65\*365/100) + (80\*365/100) + (50\*365/100) + (50\*365/100) + (50\*365/100)] / 19 = 227 | 40,000,000\*.25 = 10,000,000 | 2,227,000,000 |
| 1D | a, k, p, q, r, t, W, X, GG, KK, LL | 25% | [ (80\*365/100) + (85\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) + (35\*365/100) + (20\*365/100) + (66\*365/100) + (80\*365/100) + (50\*365/100)] / 11 = 264 | 26,000,000\*.25 = 6,500,000 | 1,716,000,000 |
| 2D | a, k, p, q, r, t, GG, KK, LL | 25% | [(80\*365/100) + (85\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) + (66\*365/100) + (80\*365/100) + (50\*365/100)] / 9 = 238 | - | - |
| 3D | a, p, q, r, t, V, W, X, Y, GG, HH, II, JJ, KK, LL, NN | 35% | [(80\*365/100) + (90\*365/100) + (80\*365/100) + (90\*365/100) + (80\*365/100) + (40\*365/100) + (10\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (66\*365/100) + (80\*365/100) + (80\*365/100) + (65\*365/100) + (80\*365/100) + (50\*365/100) + (50\*365/100)] / 17 = 221 | - | - |
| 1E | - | 20% | - | 40,000,000\*.20 = 8,000,000 | - |
| 1F | - | 15% | - | 30,200,000\*.15 = | - |
| 1G | CC | 20% | (35\*365/100) = 128 | 20,050,000\*.20 = 4,010,000 | 513,280,000 |
| 1H | V, DD | 20% | [(10\*365/100) + (66\*365/100)] / 2 = 139 | 56,500,000\*.20 = 11,300,000 | 1,570,700,000 |
| 1I | W, X, CC | 20% | [(35\*365/100) + (20\*365/100) + (35\*365/100)] / 3 = 110 | 20,400,000\*.20 = 4,080,000 | 448,800,000 |
| 1J | V, Y, Z, BB, CC, DD, EE, FF, GG, HH, II, KK, LL, NN | 15% | (10\*365/100) + (40\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) / 14 = 107 | 22,205,000\*.15 = 3,330,750 | 356,390,250 |
| 2J | V, Y, Z, BB, CC, DD, EE, FF, GG, HH, II, KK, LL, NN | 15% | (10\*365/100) + (40\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) / 14 = 107 | - | - |
| 3J | V, Z, BB, CC, DD, EE, FF | 15% | (10\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) / 7 = 100 | - | - |
| 4J | V, Z, CC, DD, EE, FF | 15% | (10\*365/100) + (35\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) + (35\*365/100) / 6 = 103 | - | - |
| 5J | V, Z, CC, DD, EE | 15% | (10\*365/100) + (35\*365/100) + (35\*365/100) + (35\*365/100) + (20\*365/100) / 5 = 99 | - | - |
| 1K | U | 10% | (35\*365/100) = 128 | 20,050,000\*.10 = 2,050,000 | 262,400,000 |
| 1L | CC | 10% | (35\*365/100) = 128 | 20,002,000\*.10 = 2,000,200 | 256,025,600 |
| 1N | r, t | 10% | - | 20,019,000\*.10 = 2,001,900 |  |

**2.3 FASE 3: REDUCCIÓN**

Se realizarán las siguientes actividades:

-Desarrollar posibles escenarios o contingencias.

-Calificar cada escenario poniendo: Que tan costoso es que suceda , que costo tendria resolverlo y cuanto tiempo tomaria.

**2.3.1 ESCENARIOS Y COSTOS**

TABLA 1 FASE 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Escenario** | **Costo** | **Acciones preventivas** | **Costo acciones preventivas** | **Tiempo estimado de corrección** |
| Existe la posibilidad que de los empleados usen las computadoras para cosas que no están relacionadas con la empresa, como bajar videos, descargar programas sin verificar su procedencia, lo cual podría traer virus o software malicioso el cual nos genere problemas con las máquinas o computadoras y retrasar las operaciones. Igual al entrar a paginas no verificadas y que por mera casualidad no haya antivirus. |  | Instalar un programa que pida una clave de acceso para poder instalar o descargar algún programa y evitar así un poco el riesgo de tener un virus. También verificar que la licencia del antivirus esté activa. | $2000 | Debe ser inmediato ya que la empresa no se puede quedar sin equipos de cómputo o maquinaria |
| Se acerca el fin de mes en el cual se le pagan salarios a los empleados así como deudas a proveedores y se le cobra a clientes, justo cuando consultan el sistema para ver cuánto se le tiene que pagar a cada quien hay una descarga eléctrica y el servidor cae, al momento de volver a levantarlo se dan cuenta de que no hay información, intentan consultar el respaldo pero no realizan respaldos periódicos y el último respaldo se realizó con errores por lo que no es útil. | $98,725,000 | Instalar una fuente de poder para evitar descargas o perdidas de energia, asi como programar respaldos frecuente de al menos 1 vez a la semana y capacitar a la persona que se va a encargar de realizar los respaldos o en su defecto automatizarlos. | $30000 | 1 semana para instalar la fuente de poder, dentro de esa semana en un par de días se pueden realizar los respaldos en automático y alrededor de 1 semana para capacitar al encargado de los respaldos. |
| Entra un nuevo interno a trabajar, se le asigna el monitoreo de la base de datos, el DBA no le asigna permisos restringidos y el interno tiene control y acceso a toda la base de datos, al ejecutar pruebas le da un drop a la base de datos, pero se da cuenta que no era su perfil y en realidad borro toda la base de datos de la empresa incluidos sus respaldos. | $98,725,000 | Limitar el acceso a la base de datos, asignar credenciales confiables y tener un respaldo en algún servidor espejo en caso de perder la base principal. | $20000 | 1 dia para asignar credenciales y una semana para montar el servidor espejo de manera óptima. |
| Se hace mal la instalación de las redes de la empresa, por lo que el sistema de seguridad queda mal configurado e inservible, un empleado en negociaciones con la compañía rival le avisa acerca del error a la otra compañía no sin antes llevarse un respaldo general para ofrecerles lo que provoca que manden gente para entrar de noche a robar y sabotear toda la compañía, dañado directo a la maquinaria y equipo de computo. | $141,557,000 | Certificar al encargado de instalar las redes para evitar fallas en las conexiones así como realizar pruebas de confianza a los empleados para descartar el espionaje organizacional. | $8000 | Dependendiendo de la duración de la certificación puede ir de 2 a 6 meses. |

**2.4 FASE 4: CONTROL**

Se realizarán las siguientes actividades:

-Explicar cómo mitigar íamos las debilidades o vulnerabilidades tomando en cuenta:

Hasta donde vamos a mitigar, Indicadores de un buen rendimiento, Quienes son los responsables?, Que se va a hacer?, Es rentable?, Establecer polìticas

· Estudiar el dominio del problema.

· Identificar aspectos positivos y negativos de la situación actual.

· Estudiar el modelo de negocio del cliente.

· Estudiar el entorno tecnológico del cliente.

· Obtener y documentar las necesidades de clientes y usuarios.

· Desarrollar los requisitos de un sistema software que satisfaga las necesidades del negocio

· Desarrollar la visión general del sistema.

· Documentar los requisitos del sistema.

· Definir las posibilidades de integración del sistema.

· Analizar los requisitos del sistema.

· Verificar la calidad de los requisitos del sistema.

· Validar los requisitos del sistema.

· Gestionar los requisitos del sistema software a desarrollar

· Definir el ciclo de vida de los requisitos del sistema.

· Gestionar las líneas base de los requisitos del sistema. Su objetivo fundamental es la generación de versiones del proyecto.

· Gestionar los conflictos de los requisitos.

· Gestionar las peticiones de cambio.

· Gestionar la trazabilidad de los requisitos del sistema.

**2.4.1 PROBLEMAS Y ACCIONES CORRECTIVAS**

Propuesta de solución:

-Hablando sobre la infraestructura

El área de IT tiene un espacio reducido para trabajar y poder tener más personal que se dedique a darle mantenimiento a algún módulo del CRM, también este problema de logística se ve reflejado en el espacio reducido que se tiene para el servidor y el equipo de redes.El área de IT tiene un espacio reducido para trabajar y poder tener más personal que se dedique a darle mantenimiento a algún módulo del CRM, también este problema de logística se ve reflejado en el espacio reducido que se tiene para el servidor y el equipo de redes.

Esta propuesta habla primero es sobre la infraestructura que debe tener la empresa, pero es parte funcional de un buen desempeño en el àrea de trabajo. Proponemos que se doble el àrea que se le da a IT no necesariamente debe ser construir una oficina extra, se puede ocupar alguna de las que ya se tienen y conectarlas mediante Redes LAN. Por otro lado dedicarle una pequeña àrea al servidor donde esté asegurado bajo llave y tenga ventilaciòn y enfriamiento para que no esté a la mano de cualquier persona.

-Hablando sobre el Sistema de Información

El sistema CRM que tienen es dedicado para manejar las relaciones con el cliente, si seguimos la definición de CRM DEBERÍA CUMPLIR con las siguientes especificaciones: Dicho software puede comprender varias funcionalidades para gestionar las ventas y los clientes de la empresa: automatización y promoción de ventas, tecnologías [data warehouse](https://es.wikipedia.org/wiki/Data_warehouse) (*almacén de datos*) para agregar la información transaccional y proporcionar capa de reporting, dashboards e indicadores claves de negocio, funcionalidades para seguimiento de campañas de marketing y gestión de oportunidades de negocio, capacidades predictivas y de proyección de ventas. El CRM que se tiene esta màs enfocado a control de Inventario y el control del proceso de facturación y seguimiento de ventas. Dado que lo que ellos buscan es integración de operaciones, lo más adecuado es un ERP que les permita tener el Sistema de control de Inventario que tiene màs las tareas que no cmple su CRM segun la definición,de esta manera se agregarían tareas como: seguimiento en marketing, seguimiento de ventas que interactúe con el cliente, el control de procesos de calidad hablando por el lado de la planta es algo que no tienen pero sería bueno monitorearlo, capacidades predictivas usando minería de datos y gestión de oportunidades de negocio. Aprovechando que su Base de datos es centralizada y eso es requerido en un ERP porque usa datos ùnicos y consistentes. De esta forma se engloba el CRM dentro del ERP.

El costo de instalar un ERP depende del grado de especialización que la empresa requiera y del tamaño de la empresa que en este caso es pequeña-mediana PYME, en nuestro caso elegiremos uno generalista, con los aspectos de seguridad mínimos, cotizamos cuanto cuesta comprar uno en Wolters Kluwer , es un a3ERP base que cuesta entre 100,000 y 400,000 pesos segùn qué tan complejo es , la cantidad de licencias que requieran, este ERP es de los que cobran menos por su costo de mantenimiento anual (la cifra es dinámica) e incluyendo capacitación, integración y soporte tècnico.

Finalmente estimamos que el implementar estas dos propuestas de solución tomaría alrededor de 6 -8 meses en estar funcionando y costaría aproximadamente $200,00 a $300,00 porque habría que suspender en algún momento el Servidor con el CRM para realizar los cambios necesarios y eso costaría pérdidas por alrededor de $100,00 si se realiza rápidamente.



**2.5 GRÁFICAS DE RIESGOS**

Se grafica la tasa de crecimiento del riesgo contra el tiempo,la gráfica de riesgo muestra la tasa de fallas instantánea para cada tiempo t.

TIPOS DE COMPORTAMIENTOS EN LOS RIESGOS

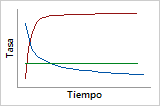
###### **Normal**

La función de riesgo es estrictamente creciente.



###### **Weibull**

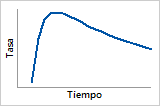
La función de riesgo puede ser constante, creciente o decreciente.

****

****

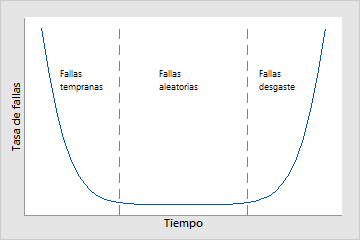
###### **Lognormal**

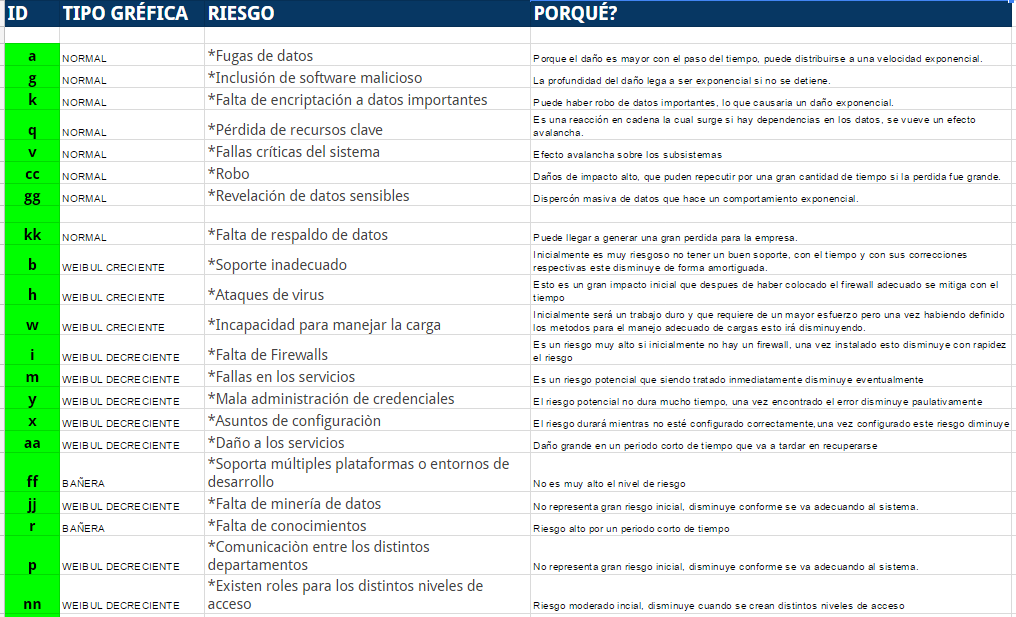
La función de riesgo aumenta hasta un máximo, luego disminuye.

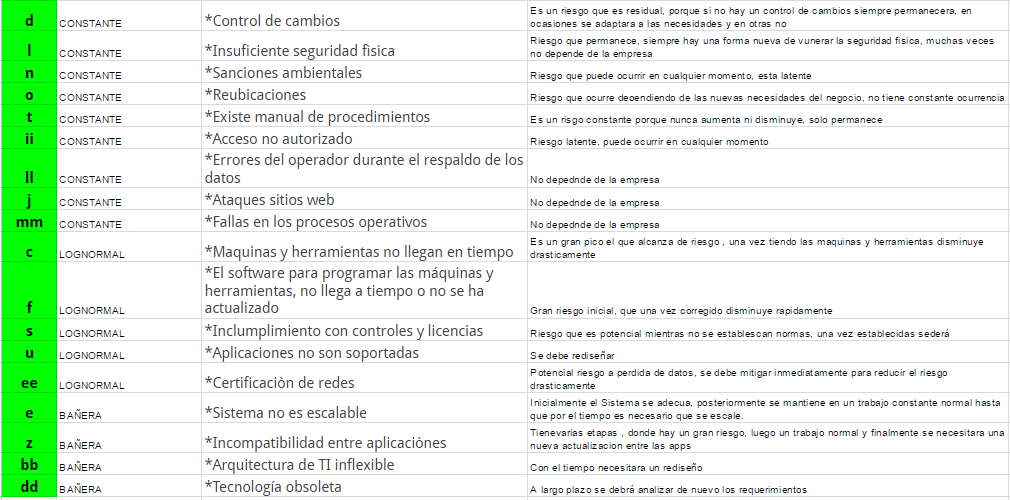


###### **Curva de bañera**

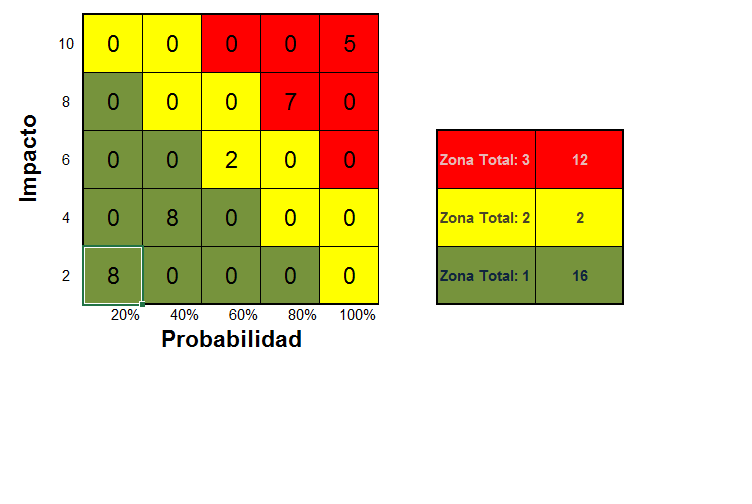
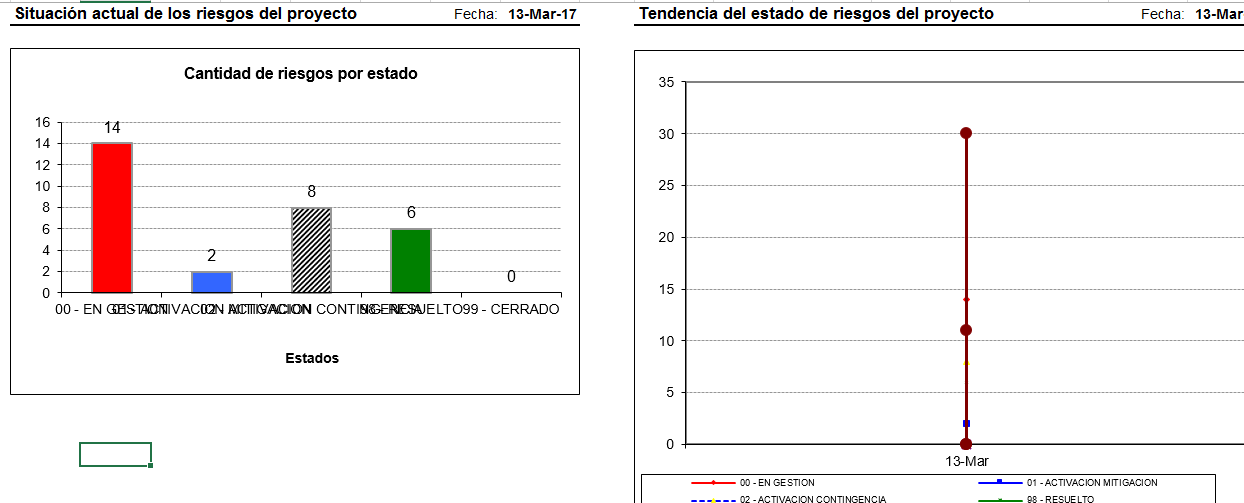
Muchos productos tienen tasas de fallas que siguen la curva de la "bañera". La tasa de riesgo suele ser alta al principio, baja en el medio y nuevamente alta al final de la vida útil. Por esa razón, la curva resultante de los tres períodos de falla frecuentemente se asemeja a la forma de una bañera. El primer período con una tasa elevada de fallas comúnmente se conoce como la etapa de fallas prematuras. El período intermedio, en el que la tasa de fallas es baja, es la etapa de vida normal. El período final, en el que la tasa de fallas vuelve a aumentar, es la etapa de desgaste.

****

****

****

**2.6 SIMULACIÓNES**



En las gráficas se puede observar la clasificación de los riesgos y el tipo de impacto que representan para la empresa, al igual que el proceso en el cual se encuentran dichos riesgos.

**3. CONCLUSIONES**

El proceso de análisis de riesgos es muy extenso y si en alguna de sus etapas no se realiza de forma organizada, esto puede llevar a un mal cálculo que nos daría falsa información acerca de qué tan impactante puede ser o no un riesgo, es por ello que hemos aprendido que tener una buena comunicación en cada fase del desarrollo del análisi de riesgos es sumamente importante.