UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

Tema:

"**POLITICAS DE SEGURIDAD Y LOS RIESGOS INFORMATICOS EN INDUSTRIA CATEDRAL S.A. DE LA CIUDAD DE AMBATO DURANTE EL AÑO 2010**"

TRABAJO DE INVESTIGACIÓN

Previo a la obtención del grado académico de

MAGÍSTER EN REDES Y TELECOMUNICACIONES

Autor: Ing. Silvia Viviana Zurita Manosalvas

Director: Ing. Mg. David Guevara Aulestia.

Ambato - Ecuador

2011

Al consejo de Posgrado de la UTA:

El tribunal receptor de la defensa del trabajo de investigación con el tema: "POLITICAS DE SEGURIDAD Y LOS RIESGOS INFORMATICOS EN INDUSTRIA CATEDRAL S.A. DE LA CIUDAD DE AMBATO DURANTE EL AÑO 2010", presentado por: Ing. Silvia Viviana Zurita Manosalvas y conformado por: Ing. Mg. Teresa Freire Aillón, Ing. Mg. Galo López Sevilla e Ing. Mg. Clay Aldás Flores, Miembros del Tribunal, Ing. Mg. David Guevara Aulestia, Director del trabajo de investigación y presidido por: Ing. M. Sc. Oswaldo Paredes Ochoa, Presidente del tribunal; Ing. Mg. Juan Garcés Chávez Director del CEPOS – UTA, una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de investigación para uso y custodia en la biblioteca de la UTA.

Ing. M. Sc. Oswaldo Paredes Ochoa
Presidente del Tribunal de Defensa

Ing. Mg. Juan Garcés Chávez
Director del CEPOS

Ing. Mg. David Guevara Aulestia
Director de Trabajo de Investigación

Ing. Mg. Teresa Freire Aillón
Miembro del Tribunal

Ing. Mg. Galo López Sevilla
Miembro del Tribunal

Ing. Mg. Clay Aldás Flores
Miembro del Tribunal

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de investigación con el tema **"POLITICAS DE SEGURIDAD Y LOS RIESGOS INFORMATICOS EN INDUSTRIA CATEDRAL S.A. DE LA CIUDAD DE AMBATO DURANTE EL AÑO 2010"**, nos corresponde exclusivamente a Ing. Silvia Viviana Zurita Manosalvas, Autor y del Ing. Mg. David Guevara Aulestia, Director del Trabajo de Investigación; y el patrimonio intelectual del mismo a la Universidad Técnica de Ambato.

Ing. Silvia Viviana Zurita Manosalvas
Autor

Ing. Mg. David Guevara Aulestia
Director

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este trabajo de investigación o parte de él un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo de investigación, con fines de difusión pública, además apruebo la reproducción de esta, dentro y fuera de las regulaciones de la Universidad.

_____

Ing. Silvia Viviana Zurita Manosalvas

DEDICATORIA

La presente tesis la dedico:

A mi señor, Jesús quien me ha dado la fortaleza la salud para seguir, sin dejarme flaquear ante los momentos difíciles de la vida.

A mi adorada hija Jéssica Gabriela quien con su amor y apoyo incondicional me ha ayudado a perseverar en cada situación

A mis padres quienes me enseñaron desde pequeña a luchar para alcanzar mis metas.

Ing. Silvia Viviana Zurita Manosalvas

AGRADECIMIENTO

Quiero expresar mi agradecimiento

A mi Director de Tesis, Ing. Mg. David Guevara Aulestia por brindarme la oportunidad de recurrir a su capacidad y experiencia en el área, en un marco de confianza, afecto y amistad, fundamentales para la concreción de este trabajo.

A mi familia por estar conmigo, en mis triunfos y fracasos, enseñándome a enfrentar los obstáculos en mi vida.

Ing. Silvia Viviana Zurita Manosalvas

ÍNDICE GENERAL

ÍNDICE DE TABLAS

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE ESTUDIOS DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES VERSIÓN II

"POLITICAS DE SEGURIDAD Y LOS RIESGOS INFORMATICOS EN INDUSTRIA CATEDRAL S.A. DE LA CIUDAD DE AMBATO DURANTE EL AÑO 2010"

Autores: Ing. Silvia Viviana Zurita Manosalvas
Tutor: Ing. Mg. David Guevara Aulestia

RESUMEN

La investigación sobre **"POLITICAS DE SEGURIDAD Y LOS RIESGOS INFORMATICOS EN INDUSTRIA CATEDRAL S.A. DE LA CIUDAD DE AMBATO DURANTE EL AÑO 2010"**, tiene como objetivo general reflexionar sobre la falta de seguridades informáticas en la información critica de Industrias Catedral, determinar los riesgos informáticos existentes, el impacto que estos causarían en la organización al materializarse, para así determinar las Políticas de seguridad informática que ayuden a salvaguardar la información.

DESCRIPTORES: Los riesgos que existen sobre los activos informáticos y las políticas que permitirán reducir los mismos.

INTRODUCCIÓN

El uso de las tecnologías de información en el mundo es cada vez mas evidente, entre sus características se destaca su comportamiento cambiante y revolucionario.

Para la mayoría de las organizaciones estar a la vanguardia de la tecnología es imprescindible, por cuanto ayuda a minimizar los procesos de una organización.

Sin embargo con el uso de la tecnología, nace la necesidad de proteger a la organización contra el mal uso interno o externo de los sistemas de cómputo o contra la intrusión de algún cracker a su sistema de red.

La falta de una cultura informática y la presencia casi nula de una legislación informática, principalmente en los países en desarrollo, trae como consecuencia riesgos a los activos informáticos de una organización

En cuanto a legislación informática, se refiere ha sido poco estudiado, por lo que campos como la protección jurídica de la información personal, protección jurídica del software, delitos informáticos entre otros de igual importancia aun están lejos de ser legislados en su totalidad.

El presente proyecto pretende determinar los riesgos en los activos informáticos y basándose en ellos proponer Políticas de Seguridad, como una forma de eliminar en lo posible los riesgos de ataque a la información de la empresa.

CAPÍTULO I, EL PROBLEMA contiene: Contextualización, Macro Contextualización, Meso Contextualización, Micro Contextualización, Análisis Crítico, Prognosis, Formulacion del Problema, Interrogantes de La Investigacion, Delimitacion de la Investigacion, Justificacion, Objetivos Generales y Especifico

El CAPÍTULO II MARCO TEÓRICO contiene: Marco Teórico, Antecedentes de la Investigacion, Fundamentaciones Filosófica Legal, Organizador Lógico de Variables, Categorías de la Variable Independiente, Categorías de la Variable Dependiente, Hipótesis o Pregunta Directriz, Señalamiento de Variables.

El CAPÍTULO III METODOLOGÍA contiene: Metodología, Modalidad de Investigación, Niveles o Tipos, Población y Muestra, Operacionalizacion de Variables, Técnicas e Instrumentos, Plan para Recolección de la Información, Plan para Procesamiento de la Información

El CAPÍTULO IV ANALISIS E INTERPRETACION contiene: Análisis e Interpretación de resultados, verificación de la hipótesis

El CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES contiene: Conclusiones y Recomendaciones del problema

El CAPÍTULO VI PROPUESTA: Antecedentes de la propuesta, Justificacion, Objetivos, General especifico, análisis de Factibilidad, Metodologia, Modelo Operativo, Conclusiones y Recomendaciones

CAPÍTULO I

EL PROBLEMA

Políticas de seguridad para reducir los riegos informáticos en Industrias Catedral S.A.

Planteamiento Del Problema

Contextualización

Macro Contextualización

A nivel Mundial el uso de tecnologías para el procesamiento de información en las organizaciones, permiten que sean objetivo fácil para las personas malintencionadas que podrían causar daños como: robar o destruir dicha información, violar la privacidad, provocar caídas del sistema, denegar servicios, modificar los datos entre otros.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del Estudio de Seguridad y Delitos Informáticos 2000 confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.

Meso Contextualización

En nuestro País, la gestión de riesgos y la seguridad informática es un fenómeno que poco se ha estudiado.

La falta de seguridad en las empresas, hacen que estas sean vulnerables a los ataques informáticos, siendo esta problemática muy común en la actualidad. De ahí que la necesidad de proteger a la información es indispensable

Micro Contextualización

Industrias Catedral, es una empresa productora y comercializadora de productos de consumo masivo de nuestra ciudad. Maneja un gran volumen de información que es esencial para el desarrollo de la misma.

Ante los crecientes ataques a la información, los altos mandos de Industrias Catedral han sentido la necesidad de proteger a la información. Razón por la cual se hace necesario establecer Políticas de Seguridad que ayuden a reducir el impacto de los riesgos en la empresa.

Análisis Crítico

Problema **Falta de seguridades en la información critica de Industrias Catedral**	
Causa	**Efecto**
El uso de tecnologías de información	La información este expuesta a posibles Ataques Informáticos
La falta de conocimientos de Seguridad Informática por parte de los usuarios	Que existan vulnerabilidades en los activos informáticos de la empresa
La falta de **Políticas de Seguridad Informática**	Aumenta el impacto de los **Riesgos Informáticos** en los activos de Industrias Catedral

Tabla 1.1: Causas que producen falta de seguridad en la información y sus posibles efectos

- El uso de tecnologías de información ayuda enormemente en los procesos de una organización, razón por la cual su uso ha aumentado y junto a ello el crecimiento de ataques informáticos se ha hecho presente, el mismo que al no ser controlado pone en riesgo los activos informáticos.

- A pesar del crecimiento de los ataques informáticos, poco se ha enfatizado en la seguridad de la información. La gran mayoría de ataques, según estudios realizados se han dado por parte de los usuarios internos a causa de la falta de conocimiento, lo que ha ocasionado un mayor número de vulnerabilidades en los activos informáticos
- La falta de Políticas de Seguridad ante los riesgos eminentes, ocasionan que aumente el impacto de estos en la organización. Razón por la cual, los altos mandos de las organizaciones deben concientizarse a tiempo de esta problemática, el no hacerlo, llevaría a la organización a no tener confiabilidad, integridad y disponibilidad de la información cuando esta sea requerida.

Prognosis

El uso de tecnologías de información para la sistematización de procesos, si bien ha sido de gran ayuda, a ocasionado incertidumbre a los altos mandos de Industrias Catedral, debido al aumento de ataques informáticos. Se ha evidenciado la falta de una cultura informática en nuestro medio, lo que ha ocasionado que estos riesgos informáticos se materialicen, generado pérdidas en las empresas. Razón por la cual Industrias Catedral ha sentido la necesidad de dar una solución al problema de la Falta de Seguridad en la Información crítica.

Formulación del Problema

¿Cómo inciden las **Políticas de Seguridad** en la **Información Crítica** de Industrial Catedral?

Interrogantes de la Investigación

- ¿Cuáles son las **Políticas de Seguridad** que se utilizan en Industrial Catedral?
- ¿A qué tipo de **Riesgos Informáticos** están expuestos los activos informáticos de Industrial Catedral?

- ¿Existen alternativas de solución al problema de la Falta de seguridad en la Información Crítica de Industrias Catedral?

Delimitación de la Investigación

Campo: Ingeniería

Área: Seguridad Informática

Aspecto: Políticas de Seguridad y Riesgos Informáticos

Delimitación Espacial:

Esta investigación se va a realizar en Industrias Catedral de la ciudad de Ambato.

Delimitación Temporal:

Este problema va a ser estudiado en el primer trimestre del 2010.

Unidades de Observación:

- Gerente y Presidente
- Jefe de Sistemas
- Personal Administrativo

JUSTIFICACION

En la actualidad, las organizaciones son cada vez más dependientes de las tecnologías de información y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las tecnologías de información es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco debe subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas.

Además de las técnicas y herramientas criptográficas, es importante recalcar que

un componente muy importante para la protección de los recursos informáticos consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la seguridad

Siendo Industrias Catedral una empresa que esta a la vanguardia de la tecnología, también se ha visto afectada por la falta de seguridades en los activos informáticos

De ahí la necesidad de proteger la información y a sus activos informáticos, evitando así que los riesgos a los cuales esta expuestos los activos informáticos se materialicen.

El presente proyecto ayudara a tener **Integridad**, **Confidencialidad, Disponibilidad** de la información cuando esta sea requerida por los altos mandos gerenciales de la empresa.

OBJETIVOS

GENERAL

Determinar las P**olíticas de Seguridad** y los **riesgos informáticos** en Industrias Catedral S.A.

ESPECIFICOS

- Determinar las **Políticas de Seguridad** que se utilizan en Industrial Catedral
- Cuantificar el impacto de los **riesgos informáticos** en Industrial Catedral
- Plantear una solución al problema de la falta de seguridad en la Información Crítica de Industrias Catedral

CAPITULO II

MARCO TEÓRICO

Antecedentes de Investigación

Para la realización del presente proyecto se ha tomado como referencia a:

- Propuesta de Políticas de Seguridad informática para la empresa FAIRIS – Sánchez Romo Karina – 2008, quien llegó a la conclusión: " Para que la información pueda ser protegida es necesario clasificar la información por la sensibilidad que puede tener esta para identificar todos los posibles riesgos "
- Implantación de un Sistema de Detección de Intrusos en la Red Informática del Centro de Experimentación y Producción Salache de la Universidad Técnica de Cotopaxi – Urrutia Urrutia Elsa Pilar - 2007

Fundamentaciones

Fundamentación Legal

La ley que rige en nuestro país para la protección de la información es la a Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Ley No. 2002-67). En la cual se menciona las consideradas infracciones informáticas y se tipifica mediante reformas a l Código Penal.

Categorías Fundamentales

Categorías de la Variable Independiente

Seguridad Informática

Seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo esta siempre presente, independiente de las medidas que tomemos, por lo que debemos hablar **de** niveles de seguridad. La seguridad absoluta no es posible.

Los niveles de seguridad permiten proteger a la información de posibles y potenciales intentos de abuso del mismo y que sea accedida única y exclusivamente por quienes tienen la autorización para hacerlo, además de alertar si existe algún cambio en él.

La seguridad tiene su nacimiento con la aparición de los ataques a la información por parte de intrusos interesados en el contenido de ésta.

Objetivos de la Seguridad Informática

Disponibilidad: Consiste en mantener la información y los recursos de acuerdo con los requisitos de utilización que requiere la entidad que proporcione la red informática. La disponibilidad de la información garantiza que no se limite el acceso autorizado a la información y el correcto funcionamiento de los recursos.

Integridad: La información que se almacena en los sistemas o que circula por las líneas de comunicación debe estar protegida contra la modificación no autorizada. Solo las entidades autorizadas pueden modificar la información.

Autenticidad: La información que se almacena o circula por una red debe permanecer protegida ante falsificaciones. La autenticidad necesita mecanismos de identificación correctos, asegurando que las comunicaciones se realizan entre entidades legítimas.

Confidencialidad: Evita la difusión no autorizada de la información. Permite que la información sea accesible únicamente por las entidades autorizadas.

- **No rechazo**: Establecer los mecanismos para que la persona que ha realizado una determinada acción no pueda negar dicha acción.

Clasificación de la Seguridad

La seguridad en un sistema podríamos clasificarla de dos modos:

Seguridad Activa

Seguridad Preventiva.

Seguridad activa de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo.

Un firewall es un buen ejemplo de seguridad activa, trata de filtrar el acceso a ciertos servicios en determinadas conexiones para evitar el intento de forzamiento desde alguno de ellos.

Seguridad preventiva es aquella que implantamos en nuestro sistema para que nos informe si en el está teniendo lugar una incidencia de seguridad. No pretende proteger el sistema, pretende alertarnos de que algo extraño está sucediendo en él. Un buen ejemplo de seguridad preventiva es un sistema de detección de intrusos.

Etapa de definición

La etapa de definición de las necesidades de seguridad es el primer paso hacia la implementación de una política de seguridad.

El objetivo es determinar las necesidades de la organización mediante la redacción de un inventario del sistema de información y luego estudiar los diferentes riesgos y las distintas amenazas que representan para implementar una política de seguridad apropiada.

Etapa de Definición de Seguridades

La etapa de definición se compone entonces de tres etapas:

- Identificación de las necesidades
- Análisis de los riesgos
- Definición de la política de seguridad

Política de Seguridad

La política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

La política de seguridad define un número de reglas, procedimientos y prácticas óptimas que aseguren un nivel de seguridad que esté a la altura de las necesidades de la organización.

Este documento se debe presentar como un proyecto que incluya a todos, desde los usuarios hasta el rango más alto de la jerarquía, para ser aceptado por todos. Una vez redactada la política de seguridad, se deben enviar a los empleados las cláusulas que los impliquen para que la política de seguridad tenga el mayor impacto posible.

El documento de Políticas de Seguridad debe contener

- Una definición de seguridad de la información, su alcance, objetivos y su importancia para garantizar el cumplimiento de la misión de la organización.
- Servicios ofrecidos (y sus riesgos) vs. seguridad proporcionada (nivel de seguridad)
- Facilidad de uso vs. seguridad
- Costos de la seguridad (monetario, rendimiento) vs. Riesgos (perdida de confidencialidad, integridad y disponibilidad).
- Determinarán que tan seguros o protegidos están los activos de información de una organización.

El éxito de una política de seguridad depende de sus objetivos, no de las herramientas utilizadas para implantar la política.

Revisión y evaluación de las políticas de seguridad de la información

La política de seguridad debe tener un responsable quien se encargue de su mantenimiento y revisión de acuerdo a un proceso predefinido que debe:

- Ejecutarse periódicamente para evaluar la efectividad de las políticas en cuanto a:

  a) la naturaleza, cantidad e impacto de los incidentes reportados y

  b) el costo e impacto de los controles sobre la efectividad del negocio.

- Ejecutarse cada vez que ocurra un evento que afecte el la seguridad de la información: nuevas vulnerabilidades, cambios en la infraestructura técnica u organizacional, ocurrencia de un incidente de seguridad significativo

Categorías de la Variable Dependiente

Identificación de Activos Informáticos – Se define como activos informáticos a todo recurso tecnológico que posee la empresa para el procesamiento de información

Servicios

Datos / Información

Aplicaciones (software)

Equipos informáticos (hardware)

Redes de comunicaciones

Soportes de información

Instalaciones

Personal

Dimensiones de valoración

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Relación de dimensiones

Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño.

La disponibilidad es una característica que afecta a todo tipo de activos.

Integridad de los datos

Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración voluntaria o intencionada, causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

Confidencialidad de los datos

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

Autenticidad de los usuarios del servicio

Aseguramiento de la identidad u origen.

¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio.

Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.

Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

Autenticidad del origen de los datos

Aseguramiento de la identidad u origen.

¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?

Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

Criterios de valoración

Para valorar los activos, teóricamente, cualquier escala de valores está bien, a efectos prácticos, es sin embargo muy importante que:

•Se use una escala común para todas las dimensiones, permitiendo comparar riesgos

• Se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas

• Se use un criterio homogéneo que permita comparar análisis realizados por separado

Amenazas

Una amenaza es cualquier cosa que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de nuestros activos.

> Causa potencial de un incidente que puede causar daño a un sistema o a una organización.
>
> [ISO/IEC 27002:2005]

Se presenta a continuación posibles amenazas sobre los activos de un sistema de información.

- **Desastres naturales**
- **De origen industrial**

  Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial.
- **Corte del suministro eléctrico**
- **Condiciones inadecuadas de temperatura y/o humedad**

  Fallo de servicios de comunicaciones
- **Deficiencias en la organización**
- **Difusión de software dañino**
- **Alteración de la información**
- **Destrucción de información**
- **Divulgación de información**
- **Vulnerabilidades de los programas (software)**
- **Caída del sistema por agotamiento de recursos**
- **Indisponibilidad del personal**
- **Robo-**
- **Destrucción de un activo**

Los activos son más o menos vulnerables a las amenazas que pueden suceder sobre ellos.

La vulnerabilidad de un activo a una amenaza se mide por medio de dos informaciones:

- la probabilidad de que ocurra
- la degradación del valor del activo

Degradación

La degradación mide la pérdida de valor de un activo cuando ocurre una amenaza.

> Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.
>
> MAGERIT

La degradación se puede medir como porcentaje: la proporción del valor del activo que se pierde cuando ocurre un incidente.

Probabilidad

Algunas amenazas son más probables que otras, por diversas razones:

- Estadística histórica (experiencia pasada o experiencia ajena)
- El activo está muy expuesto
- Hay un elevado número de ataques posibles con bastante potencial del ataque
- El atacante conseguiría un beneficio elevado

Impacto

El impacto es la medida del daño causado por una amenaza cuando se materializa sobre un activo.

Impacto
Consecuencias para la Organización cuando se materializa una amenaza. [EBIOS: 2005]

Sabiendo el valor de los activos, y la degradación causada por las amenazas, se estima el impacto como:

impacto = valor - degradación

Impacto residual

Las salvaguardas reducen la probabilidad de que ocurra o no, la degradación causada en el activo.

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

Impacto residual
El impacto restante después del tratamiento del riesgo.

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
- la degradación causada por la amenaza

impacto_acumulado = valor_acumulado – degradación

Riesgo

El riesgo es el daño que se repite, causado por incidentes que se repiten.

Sabiendo el impacto de una amenaza y su probabilidad, se estima el riesgo como:

riesgo = impacto * probabilidad

Riesgo residual

Las salvaguardas reducen la probabilidad de que una amenaza ocurra o la degradación derivada de su materialización.

Cuando en la evaluación del riesgo utilizamos los valores residuales para la probabilidad y la degradación (es decir, los valores originales reducidos por la eficacia de las salvaguardas), entonces el resultado es el riesgo residual.

Riesgo residual
Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.
[ISO Guide73: 2002]

Riesgo acumulado

El riesgo acumulado se calcula tomando en consideración el valor acumulado y el efecto directo de las amenazas sobre el activo.

Puesto que hay dependencias entre activos, los activos inferiores acumulan el valor de los activos superiores.

El riesgo acumulado es la valoración del daño para la organización, evaluado en los activos inferiores.

Para calcular el riesgo acumulado que utilizamos

- el impacto acumulado
- la probabilidad

riesgo_acumulado = impacto_acumulado – probabilidad

De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos tipos de consecuencias: ganancias o pérdidas.

En lo relacionado con tecnología, generalmente el riesgo se plantea como una amenaza, determinando el grado de exposición a la ocurrencia de una pérdida

Por ejemplo:

El riesgo de perder datos debido a rotura de disco, virus informáticos, etc.

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996) como:

La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños.

Las amenazas sobre los activos son una fuente de daño que, si no es protegido, ocurre una y otra vez.

Análisis de Riesgos Informáticos

El **Análisis de Riesgos de Seguridad Informática** es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo. Se debe mostrar los elementos identificados, la manera en que se relacionan y los cálculos realizados. El análisis de riesgo es indispensable para lograr una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización.

El activo más importante que posee una organización, es la información y por lo tanto, deben existir técnicas que la aseguren.

Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: "lo que no está permitido debe estar prohibido" y ésta debe ser la meta perseguida.

Existen una serie de diferentes enfoques para el análisis de riesgos pero, en esencia, suelen dividirse en dos tipos fundamentales: cuantitativos y cualitativos.

Enfoque Cuantitativo de Análisis de Riesgos

Este enfoque emplea dos elementos fundamentales:

- la probabilidad de que se produzca un hecho

- la probable pérdida en caso de que ocurra el hecho citado.

El enfoque cuantitativo de análisis de riesgos se centra en el uso de una sola cifra producida a partir de estos elementos. A esto se le suele denominar comúnmente el "Annual Loss Expectancy" – ALE (Esperanza de pérdida anual) o también "Estimated Annual Cost" – EAC (Coste anual estimado). La forma de calcularlo para un evento en concreto se realiza mediante la multiplicación de la pérdida potencial por la probabilidad. Gracias a este enfoque, es teóricamente posible clasificar los acontecimientos en orden de riesgo (ALE) a fin de tomar decisiones sobre esta base.

Los problemas con este tipo de análisis de riesgos están generalmente asociados con la inexactitud y falta de fiabilidad de los datos.

Los datos asociados a las probabilidades estimadas por lo general bajo el criterio interno de la empresa rara vez suelen ser precisos y pueden, en algunos casos, estar basados en la propia autocomplacencia de los dueños de los procesos de

negocio. Además, los controles y las contramedidas a menudo hacen frente a una serie de posibles acontecimientos en los que los hechos que los producen están normalmente interrelacionados.

A pesar de estos inconvenientes, son numerosas las organizaciones que han adoptado y aplicado con éxito el análisis de riesgo cuantitativo.

Enfoque Cualitativo de Análisis de Riesgos

Es la metodología más utilizada para el análisis de riesgos. En este caso, la probabilidad no es necesaria y tan solo es utilizado como factor de cálculo la pérdida potencial estimada.

Evaluación de los Riesgos

Después de efectuar el análisis debemos determinar las acciones a tomar respecto a los riesgos residuales que se identificaron. Las acciones pueden ser:

- **Controlar el riesgo.-** Fortalecer los controles existentes y/o agregar nuevos controles.
- **Eliminar el riesgo.-** Eliminar el activo relacionado y con ello se elimina el riesgo.
- **Compartir el riesgo.-** Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.
- **Aceptar el riesgo.-** Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

Hipótesis o Pregunta directriz

Las Políticas de Seguridad Informática ayudaran a reducir los riesgos informáticos en Industrias Catedral

Señalamiento de Variables

Variable Independiente: Políticas de Seguridad

Variable Dependiente: Riesgos Informáticos

CAPITULO III

METODOLOGÍA

Enfoque

El enfoque que tendrá el proyecto es cualitativo por cuanto este modelo busca la valoración relativa del riesgo que corren los activos sin cuantificarlo con precisión más allá de relativizar los elementos del modelo

Modalidad de Investigación

Para la elaboración del presente trabajo se utilizaran varias modalidades tales como:

- Investigación de Campo, debido que se realiza la investigación en el lugar en el que se presenta el problema. Recolectando información mediante el método de observación directa en la empresa y a través de encuestas al personal de la misma.
- Investigación documental-bibliográfica, ya que se adquirido conocimientos sobre el tema en libros, folletos, publicaciones.
- Modalidades Especiales

Niveles o Tipos

Investigación Exploratoria – Debido que es una metodología muy flexible que permite investigar un problema, clasificar, ordenar, analizar e interpretarlos los datos encontrados en ella.

En el presente trabajo nos ayudara a determinar las Políticas de Seguridad Informática para reducir los riesgos que afectan a los activos informáticos de Industrias Catedral S.A.

Investigación Descriptiva – Permitirá determinar las Políticas de Seguridad existentes en Industrias Catedral

Asociación de Variables – En el presente trabajo asociaremos la variable independiente con la variable independiente.

Población y Muestra

Industrias Catedral cuenta con el siguiente personal al que le realizaremos la encuesta:

- Gerente y Presidente 2
- Jefe de Sistemas 1
- Personal Administrativo 18

Siendo 21 en total las personas la población y la muestra.

Operacionalización de Variables

Variable Independiente:

Conceptualización	DIMENSIONES	INDICADORES	ITEMS BASICOS	TECNICAS E INSTRUMENTOS
Políticas de Seguridad de la Información - Se puede considerar como reglas, medidas o actividades destinadas a prevenir, proteger y resguardar los activos informáticos de una organización. Siendo controlado su cumplimiento por el responsable de la seguridad informática.	Reglas, Medidas o Actividades	Alto Medio Bajo	El nivel de Seguridad Informática que existe en Industrias Catedral es:	Encuesta - Cuestionario al Departamento de Sistemas
		Escaneo de Puertos Monitorización de la red Auditoria de los Equipos Informáticos Sistemas de Detección de Intrusos Ninguna	En Industrias Catedral se realizan actividades de Seguridad Informática como:	Encuesta - Cuestionario al Departamento de Sistemas
		Capacitación al Personal sobre incidencias de Seguridad Acuerdos de Confidencialidad entre La empresa y el empleado Procesos Disciplinarios para quienes violen la seguridad Controles de Acceso a la Información	Existe actividades ligadas al personal como:	Encuesta- Cuestionario al Departamento de Sistemas

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Políticas de Seguridad de la Información - Se puede considerar como reglas, medidas o actividades destinadas a prevenir, proteger y resguardar los activos informáticos de una organización. Siendo controlado su cumplimiento por el responsable de la seguridad informática.	Prevenir, Proteger y Resguardar	La empresa Fuera de la empresa Ninguna Ambos	La información importante de la empresa es respalda en :	Encuesta - Cuestionario al Departamento de Sistemas
		Temperatura Adecuada Sistema de Alarma (humo,fuego, etc) Fuentes de protección de Corriente Eléctrica Extintores de Incendio Ninguno	El área de los equipos informáticos esta implementada con:	Encuesta - Cuestionario al Departamento de Sistemas
		Preventivo Correctivo Ninguno	Existe en Industrias Catedral un Plan de Mantenimiento	Encuesta - Cuestionario al Departamento de Sistemas

Conceptualización	Dimensiones	Indicadores	Ítems básicos	Técnicas e Instrumentos
Políticas de Seguridad de la Información - Se puede considerar como reglas, medidas o actividades destinadas a prevenir, proteger y resguardar los activos informáticos de una organización. Siendo controlado su cumplimiento por el responsable de la seguridad informática.	Prevenir, Proteger y Resguardar	Dados de Baja Reutilizados Archivados Ninguno	Los soportes de Información que ya no se utiliza son:	Encuesta - Cuestionario al Departamento de Sistemas
	Activos Informáticos	Servicios Datos/Información Aplicaciones Equipos Informáticos Redes de Comunicación Soportes de Información Instalaciones No Existe Clasificación	Los activos informáticos están clasificados en base a:	Encuesta - Cuestionario al Departamento de Sistemas

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Políticas de Seguridad de la Información - Se puede considerar como reglas, medidas o actividades destinadas a prevenir, proteger y resguardar los activos informáticos de una organización. Siendo controlado su cumplimiento por el responsable de la seguridad informática.	Activos Informáticos	Disponibilidad Integridad Confidencialidad Autenticidad No existe Valoración	El criterio de Valoración de los activos esta dado en base a:	Encuesta - Cuestionario al Departamento de Sistemas
		Ubicación Responsable Fecha de Entrega Características del Equipo No existe Registro	El registro de un Activo Informático contiene datos como:	Encuesta - Cuestionario al Departamento de Sistemas

VARIABLE DEPENDIENTE

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Riegos Informáticos - Se plantea solamente como la amenaza que existe a los activos informáticos, determinando el grado de exposición a la ocurrencia de una pérdida	Amenazas	SI NO	¿Se le ha capacitado sobre las medidas de seguridad informática existentes en la empresa?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		SI NO	¿Está instalado en su equipo algún programa de protección de la información?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		Semanal Mensual Automáticamente	¿Cada qué tiempo se actualiza el antivirus en su máquina?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		Alterada Borrada Ninguna	¿En algún momento, la información que Ud. maneja fue:	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
	Activos Informáticos	SI NO	¿Se le ha mencionado sobre los cuidados que debe darle al equipo de computo que está a su cargo?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información

Conceptualizacion	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Riegos Informáticos - Se plantea solamente como la amenaza que existe a los activos informáticos, determinando el grado de exposición a la ocurrencia de una pérdida	Activos Informáticos	SI NO	¿En alguna ocasión su equipo se ha dañado y ha perdido información relevante de su proceso?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		SI NO	¿Ha instalado programas aplicaciones a los previamente instalados en su equipo?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
	Grado de Exposición de los Activos Informáticos	SI NO	¿Ud. puede acceder a la información que se encuentre en los equipos de la red o unidades compartidas?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		SI NO	¿Desde el momento que le asignaron un equipo de computo, fue creado su usuario de ingreso al equipo?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		SI NO	¿Ud. puede acceder a la información que se encuentra en los servidores centrales?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		SI NO	¿Le hablaron sobre la confidencialidad que debe existir en el manejo de una contraseña y de la responsabilidad que ésta conlleva?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información
		SI NO	¿Tiene conocimiento Ud. sobre una incidencia de seguridad de la información en la empresa?	Encuesta - Cuestionario a los usuarios de los Sistemas de Información

Técnicas e Instrumentos

Encuesta – Cuestionario

Entrevista – Guía de la entrevista

Observación – Ficha de la observación, otros

Plan para Recolección de la Información

Para la realización del presente trabajo se utilizaran las siguientes técnicas e instrumentos

- Observación

  Tipo de Observación: Directa

  Por la actitud frente a lo observado: participante

  Por la metodología utilizada: estructurada

  Por el lugar de observación: de campo

  Según quien observa: Intrasubjetiva

  Instrumentos para el registro de datos: Cuaderno de Notas

- Encuesta
- Entrevista

Plan para el Procesamiento de la Información

- Revisión critica de la información recogida
- Tabulación de las respuestas de la encuesta aplicada al personal administrativo de Industrias Catedral S.A
- Análisis e Interpretación de los resultados de la encuesta y de la entrevista

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Entrevista dirigida a: Jefe de Sistemas

Pregunta 1:

¿Qué herramientas se han instalado para garantizar seguridad en la información?

Respuesta

Se ha instalado:

NOD32 – Antivirus para evitar el daño en los datos de la organización

Look Lan – Escanea que IP están activas para determinar que maquinas están conectadas a la red

Interpretación:

Se puede determinar que se utilizan herramientas para proteger la información en un mínimo porcentaje. Las herramientas que generalmente se usan para la seguridad de la información son:

Monitoreo de la red

Escaneo de puertos

Auditoria Informática

Detección de Intrusos

Firewall y Antivirus

Pregunta 2

¿Que actividades de seguridad informática, ligadas al personal se realizan?

Respuesta

En lo referente al sistema de datos, los usuarios tienen el acceso limitado a los módulos q manejan cada uno

Interpretación:

Si bien el acceso limitado a los módulos informáticos es una actividad ligada al personal no es suficiente por cuanto se hace indispensable también:

Capacitación al Personal sobre incidencias de Seguridad

Acuerdos de Confidencialidad entre la empresa y el empleado

Procesos disciplinarios para quienes violen la seguridad

Pregunta 3

¿Qué mecanismo de backup se utiliza en Industrias Catedral para respaldar la información?

Respuesta

- Existe un servidor denominado servidor backup en donde se replica los datos del sistema y de las bases de datos
- También se replica las bases de datos y las aplicaciones en un disco externo
- En el servidor backup existe configurado un Disco Raid para bases de datos y aplicaciones

Interpretación

Si bien se utiliza 3 formas de backups para respaldar aplicaciones y bases de datos, se debería respaldar la información fuera de la empresa para prevenir perdidas por desastres naturales.

Pregunta 4

¿Existe en Industrias Catedral un Plan de Mantenimiento?

Respuesta

Existe un plan de mantenimiento preventivo cada dos meses, el mantenimiento correctivo es realizado cada vez que se lo necesita.

Interpretación

Si existe un plan de mantenimiento en un 100%

Pregunta 5

¿Con que protecciones se encuentra implementada el área de los equipos informáticos?

Respuesta

Se usa UPS para los servidores centrales y 4 equipos de los usuarios.

Interpretación

En las áreas donde se encuentran los Servidores Centrales que almacenan la mayor parte de información valiosa de la empresa, generalmente es necesario que exista protecciones esenciales como:

Controles físicos de entrada

Protección frente a incendios

Control de temperatura

Pregunta 6

¿Que documentos de Seguridad Informática se utiliza en la empresa?

Respuesta

Procedimiento para realizar copias de seguridad de bases datos y aplicaciones

Procedimiento para realizar restauración de las copias de seguridad

Interpretación

Ante posibles eventualidades se vuelve indispensable documentar todos los procedimientos que se realizan en lo referente a Seguridad Informática. Esto permitirá que la empresa siga su curso normal a pesar de las situaciones que pueden presentarse.

Pregunta 7

¿En base a que parámetros se ha determinado una clasificación de los activos informáticos?

Respuesta

No existe una clasificación de los activos informáticos

Interpretación

Al no existir una clasificación de los activos informáticos de la empresa, implica que se dé el mismo trato a todos los activos. Se debe tomar en cuenta que el activo informático más importante y sensible de una empresa es la información, como tal la mayoría de actividades de seguridad que se realicen en una empresa debe estar encaminada a cumplir con los objetivos básicos de la seguridad informática, como son mantener la integridad, confidencialidad, disponibilidad, Autenticidad en la información.

Pregunta 8

¿Se ha establecido un criterio para valor los activos informáticos de la empresa?

Respuesta

No existe un criterio de valoración

Interpretación

Es necesario ayudarse de criterios de valoración de los activos informáticos de la empresa, para proteger a los mismos en base a los requerimientos, al no existir se pone en riesgo los activos más importantes de la empresa como es la información

Encuesta dirigida a: Personal Administrativo de Industrias Catedral

Pregunta Nº 1

¿Se le ha capacitado sobre las medidas de seguridad informática existentes en la empresa?

Opciones	Frecuencia	Porcentaje
SI	0	0%
NO	21	100%
Total:	21	**100**%

Cuadro 4.1: Porcentaje de capacitación en medidas de seguridad informática

Elaborado por: Silvia Viviana Zurita M.

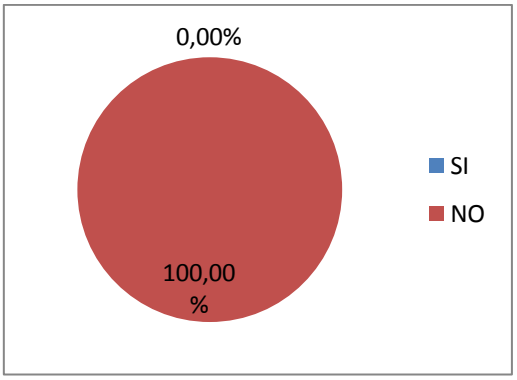


Gráfico 4.1: Porcentaje de capacitación en medidas de seguridad informática

ANÁLISIS E INTERPRETACIÓN

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 0% contesto que **SI** y un 100% contesto que **NO** existe capacitación sobre medidas de seguridad.

El porcentaje predominante es el NO

Según estudios realizados por responsables de Seguridad Informática en empresas americanas, de 516 ataques informáticos registrados, 216 corresponden a ataques informáticos realizados por parte del empleado.

Razón por la cual se vuelve indispensable capacitar al personal sobre las seguridades informáticas.

Pregunta Nº 2

¿Según la ubicación en la que se encuentra su equipo podría estar expuesto a?

Opciones	Frecuencia	Porcentaje
Polvo	14	66.67
Filtraciones de agua	0	0
Robo		
Ninguno	6	28.57
	1	4.76
Total:	21	**100**%

Cuadro 4.2: Porcentaje de riesgos en los equipos informáticos a causa de áreas inadecuadas

Elaborado por: Silvia Viviana Zurita M.

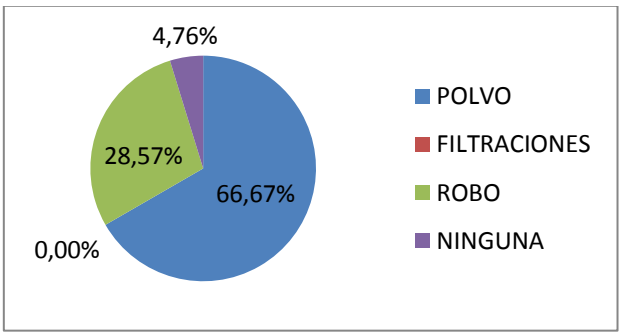


Gráfico 4.2: Porcentaje de riesgos en los equipos informáticos a causa de áreas inadecuadas

ANÁLISIS E INTERPRETACIÓN

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 66.67% contesto que existe excesivo polvo, el 0% contesto que existe filtraciones de agua, un 28.57% contesto que existe riesgo de robo y un 4.76% contesto que no existe ninguno de los riesgos expuestos.

El porcentaje predominante es el 66.67%.

Un alto porcentaje, evidencia que se debe tomar medidas correctivas y preventivas para proteger los equipos del excesivo polvo, tratando así de disminuir el índice de riesgos ante posibles daños en los equipos y eminentes pérdidas de información.

También se debe considerar que un 28.57% nos indica que los equipos pueden estar expuestos a posibles robos y junto con ellos fuga de información valiosa para la empresa.

Pregunta Nº 3

¿En algún momento su información fue alterada, borrada, copiada sin su autorización?

Opciones	Frecuencia	Porcentaje
Alterada	5	23.81%
Borrada	5	23.81%
Copiada	5	23.81%
Ninguna	6	28.57%
Total:	21	**100**%

Cuadro 4.3: Porcentaje de riesgos en la información confidencial de cada usuario
Elaborado por: Silvia Viviana Zurita M.

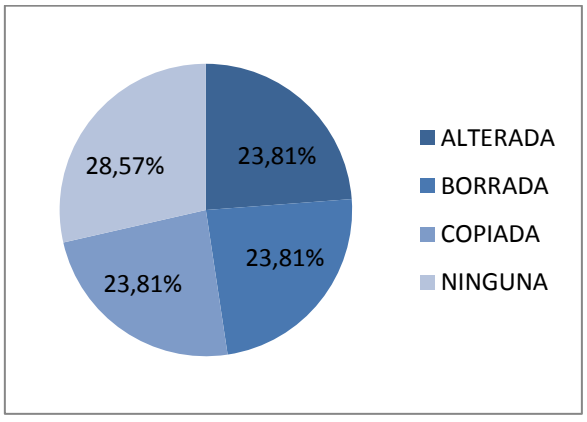


Gráfico 4.3: Porcentaje de riesgos en la información confidencial de cada usuario

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 23.81%

contesto que la información fue alterada, el 23.81% contesto que la información fue borrada, un 23.81% contesto que la información fue copiada y un 28.77% contesto que no existe ninguno de los riesgos expuestos.

El 73.41% indica que la información fue alterada, borrada o copiada por terceras personas, siendo estas empleados propios de la empresa o intrusos externos como hackers, crackers etc. que acceden a la red por falta de seguridades, incumpliendo así los objetivos básicos de la Seguridad Informática como son confidencialidad, integridad, disponibilidad, autenticidad.

Pregunta Nº 4

¿Se le ha capacitado sobre los cuidados que debe darle al equipo de cómputo que esta a su cargo?

Opciones	Frecuencia	Porcentaje
SI	12	57.14
NO	9	42.86
Total:	21	**100**%

Cuadro 4.4: Porcentaje de capacitación sobre la protección que se debe dar a los equipos para evitar posibles riesgos

Elaborado por: Silvia Viviana Zurita M.

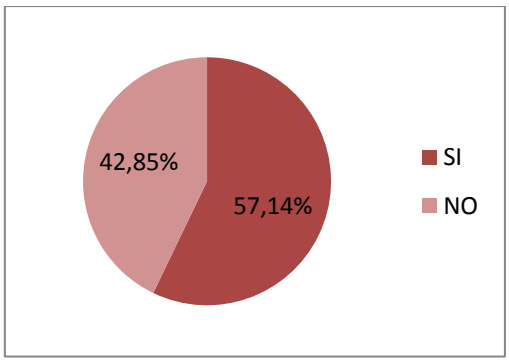


Grafico 4.4: Porcentaje de capacitación sobre la protección que se debe dar a los equipos para evitar posibles riesgos

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 57.14% contesto que SI a la pregunta formulada, el 42.85% contesto que NO tuvo una capacitación sobre la protección que se debe dar a los equipos informáticos.

El 57.14% quienes respondieron que si se les indico sobre las protecciones que se debe dar a los equipos, no ponían en practica dichas protecciones. De ahí que se evidencia que los riesgos a los equipos informáticos provienen en gran parte de los usuarios internos de la empresa.

La falta de un responsable de Seguridad Informática que se encargue de controlar que se cumpla reglas básicas de seguridad, ocasione que aumenten los riesgos informáticos.

Pregunta Nº 5

¿Ha perdido información relevante de su proceso a causa de daños en el equipo de cómputo?

Opciones	**Frecuencia**	**Porcentaje**
SI	10	47.62
NO	11	52.38
Total:	21	**100**%

Cuadro 4.5: Porcentaje de perdida de información a causa de daños en el equipo

Elaborado por: Silvia Viviana Zurita M.

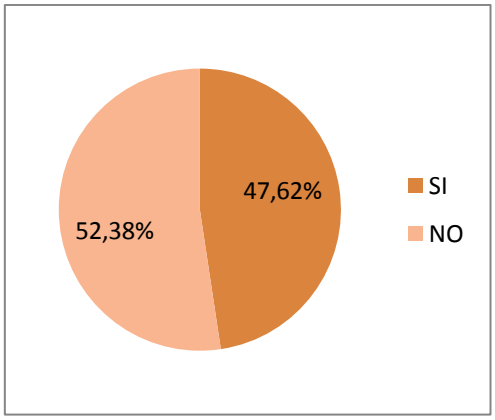


Grafico 4.5: Porcentaje de perdida de información a causa de daños en el equipo

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 47.62% contesto que SI a la pregunta formulada, el 52.38% contesto que NO ha perdido información relevante de su proceso a causa de daños en el equipo.

El porcentaje predominante es el NO con el 52.38%.

A pesar que el porcentaje predominante es el NO, no se debe dejar de lado el porcentaje que contesto que SI.

El análisis de riesgos es una actividad prioritaria de la Seguridad Informática por cuanto ayuda a reducir los riesgos a los cuales están expuestos los activos informáticos de una empresa y considerar posibles soluciones que contrarresten estos riesgos.

Pregunta Nº 6

¿Ha instalado aplicaciones adicionales a los previamente instalados en su equipo

Opciones	Frecuencia	Porcentaje
SI	9	42.86
NO	12	57.14
Total:	21	**100**%

Cuadro 4.6: Porcentaje de Instalación de programas sin autorización

Elaborado por: Silvia Viviana Zurita M.

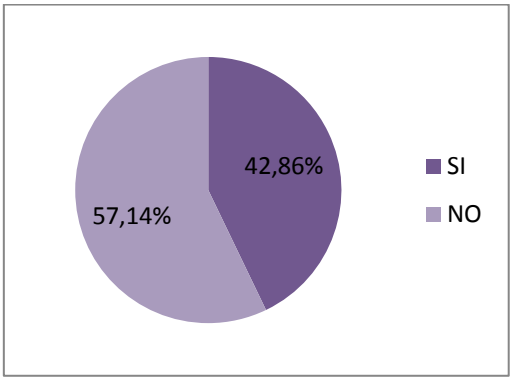


Grafico 4.6: Porcentaje de Instalación de programas sin autorización

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 42.86% contesto que SI a la pregunta formulada, el 57.14% contesto que NO ha instalado aplicaciones adicionales en el equipo.

El porcentaje predominante es el NO con el 57.14%.

El riesgo al cual pueden estar expuestos los activos informáticos aumenta al dejar abierta la posibilidad de que los usuarios instalen software, por cuanto muchos de de las aplicaciones que instalen pueden no proceder de fuentes confiables que garanticen que están libres de virus. Por tal razón a pesar de que el porcentaje predominante es el No, no se debe descuidar el porcentaje que contesto que SI ha instalado aplicaciones adicionales en sus equipos.

Pregunta Nº 7

¿Ud. a accedido a la información que se encuentra en los equipos de la red o unidades compartidas?

Opciones	Frecuencia	Porcentaje
SI	9	42.86
NO	7	33.33
Ninguno	5	23.81
Total:	21	**100**%

Cuadro 4.7: Porcentaje de controles de acceso lógico

Elaborado por: Silvia Viviana Zurita M.

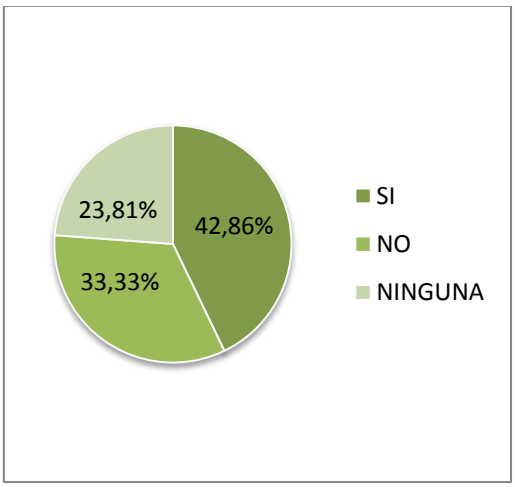


Grafico 4.7: Porcentaje de controles de acceso lógicos

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 42.86% contesto que SI a la pregunta formulada, el 33.33% contesto que NO, un 23.81contesto ninguna. Las personas que contestaron ninguna hicieron referencian a que nunca lo habían intentado o que no tenían los conocimientos necesarios para acceder a los equipos de la red o unidades de red compartidas.

La unidad compartida es una unidad del servidor central en la cual se encuentran todo los sistemas que se manejan en la empresa. Al ser información tan valiosa para la empresa debería ser restringida para usuarios comunes, debido a que podrían alterar, borrar o copiar información.

A pesar de que el porcentaje de usuarios que accedido a las unidades compartidas o equipos de la red no es alto, es suficiente para que puedan alterar la información.

Pregunta Nº 8

¿Desde el momento que le asignaron un equipo de computo fue creado su usuario y contraseña de ingreso al equipo

Opciones	Frecuencia	Porcentaje
SI	11	52.38
NO	10	47.62
Total:	21	**100**%

Cuadro 4.8: Porcentaje de restricciones de ingreso al equipo

Elaborado por: Silvia Viviana Zurita M.

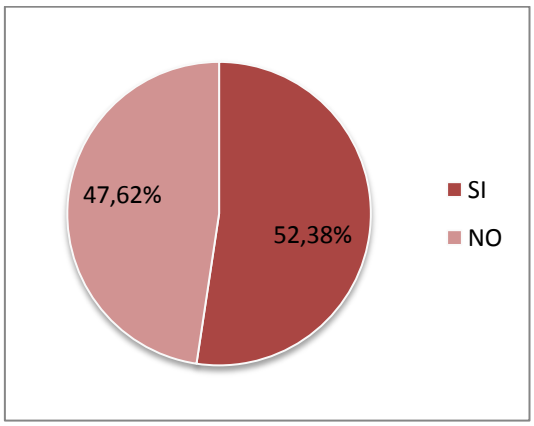


Grafico 4.8: Porcentaje de restricciones de ingreso al equipo

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 52.38% contesto que SI a la pregunta formulada, el 47.62% contesto que NO.

El porcentaje predominante es el SI con el 52.38%, esto nos indica que existe una política de asignación de usuarios y contraseñas pero no involucra a todo el personal de la empresa, ya que un 47.62% no tiene usuario de ingreso al equipo.

Una de las debilidades mas aprovechadas por los intrusos informáticos es la falta de un esquema de usuarios y contraseñas en la que abarque a todo el personal.

Otra de las debilidades que aprovechan los intrusos son los usuarios ya no se utilizan y no han sido dado de baja.

Pregunta Nº 9

¿Ud. puede acceder a las áreas donde se encuentran los servidores centrales?

Opciones	Frecuencia	Porcentaje
SI	21	100
NO	0	0
Total:	21	**100**%

Cuadro 4.9: Porcentaje de Controles de Acceso Físico

Elaborado por: Silvia Viviana Zurita M.

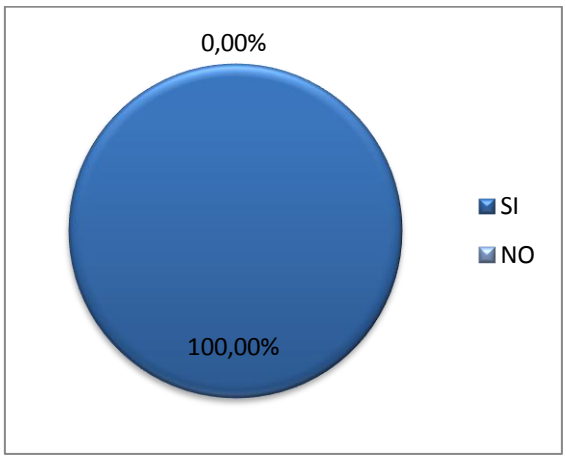


Grafico 4. 9: Porcentaje de Controles de Acceso Físico

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 100% contesto que SI a la pregunta formulada, el 0% contesto que NO.

El porcentaje predominante es el SI con el 100%

El área donde se encuentran los servidores centrales según la norma ISO 2005 debe ser implementada con:

Protecciones contra incendios

Controles de acceso físico de entrada

Instalaciones adecuadas contra el polvo

Controles de temperatura

Fuentes de protección de corriente eléctrica

La falta de estas protecciones incrementa el riesgos de perdida de información y por ende perdidas para la empresa.

Pregunta Nº 10

¿Le hablaron sobre la confidencialidad que debe existir en el manejo de una contraseña y de la responsabilidad que esta conlleva

Opciones	Frecuencia	Porcentaje
SI	3	14.29
NO	18	85.71
Total:	21	**100**%

Cuadro 4.10: Porcentaje de capacitación sobre confidencialidad en las contraseñas
Elaborado por: Silvia Viviana Zurita M.

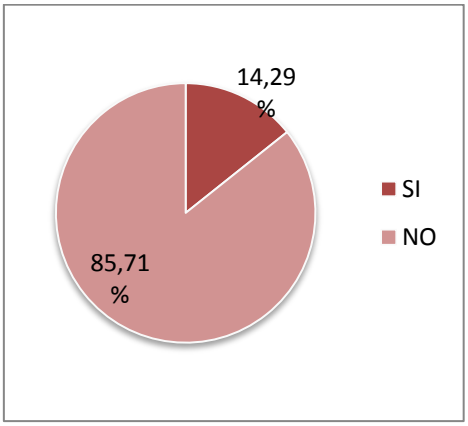


Grafico 4.10: Porcentaje de capacitación sobre confidencialidad en las contraseñas

Análisis e Interpretación

En cuanto a los porcentajes obtenidos mediante la encuesta aplicada al personal administrativo de Industrias Catedral, podemos evidenciar que un 14.29% contesto que SI a la pregunta formulada, el 85.71% contesto que NO.
El porcentaje predominante es el NO con el 100%
Los usuarios de ingreso y las contraseñas deben ser confidenciales, esto ayudara a proteger a la información.

Verificación De Hipótesis

Formulación de la hipótesis

H_0= Hipótesis nula

H_1 = Hipótesis alterna

H_0= El mejoramiento en la calidad del servicio al cliente, **no** permitirá incrementar las ventas en la empresa Industrias Catedral S.A., de la ciudad de Ambato.

H_1 = El mejoramiento en la calidad del servicio al cliente, **si** permitirá incrementar las ventas en la empresa Industrias Catedral S.A., de la ciudad de Ambato.

Definición del nivel de significación

El nivel de significación escogido para la investigación es del 5%.

Elección de la prueba estadística

Para la verificación de la hipótesis se escogió la prueba Ji Cuadrada, cuya fórmula es la siguiente:

$$\mathbf{X^2} = \frac{\Sigma\ (fo - fe)^2}{fe}$$

Simbología

Fo = Frecuencia observada

Fe = Frecuencia esperada

Para realizar la matriz de tabulación cruzada se toma en cuenta 2 preguntas del cuestionario como se muestra a continuación:

Pregunta N°5

¿A perdido

informació

n relevante de su proceso a causa de daños en el equipo de computo

SI

NO

Pregunta Nº 9

¿Ud. puede acceder a las áreas donde se encuentran los servidores centrales?

SI

NO

4.2.4 Zona de aceptación o rechazo

Grados de libertad

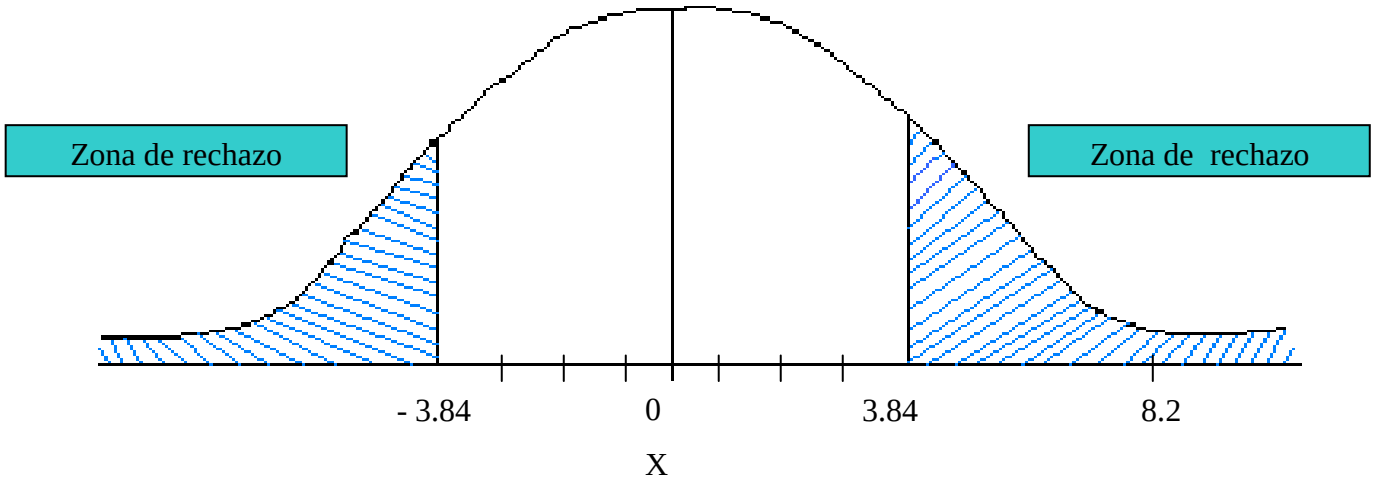
(gl) = (F-1) (C-1)

(gl) = (2-1) (2-1)

(gl) = (1) (1)

(gl) = 1

El valor tabulado de X^2 con 1 grado de libertad y un nivel de significación de 0,05 es de 3.84.



VALORES REALES

ALTERNATIVAS	ALTERNATIVAS		TOTAL
	SI	NO	
Perdida de Información por daños en el equipo	10	11	**21**
Acceso a las áreas de los servidores centrales	21	0	**21**
TOTAL	**31**	**11**	**42**

$$fe = \frac{(Total\ o\ marginal\ de\ renglon)(total\ o\ marginal\ de\ columna)}{N}$$

FRECUENCIA ESPERADA

ALTERNATIVAS	ALTERNATIVAS	
	SI	NO
CLIENTES INTERNOS	15.5	5.5
CLIENTES EXTERNOS	15.5	5.5

Una vez obtenidas las frecuencias esperadas, se aplica la siguiente fórmula:

Cálculo Matemático

$X^2 = \sum \frac{(O-E)^2}{E}$	O	E	0 - E	$(O - E)^2$	$\frac{(O - E)^2}{E}$
CLIENTES INTERNOS / SI	10	15.5	-5.5	30.25	1.95
CLIENTES INTERNOS / NO	11	5.5	5.5	30.25	5.50
CLIENTES INTERNOS / SI	21	15.5	5.5	30.25	1.95
CLIENTES EXTERNOS / NO	0	5.5	-5.5	30.25	5.50

x^2 = 14.90

Decisión

El valor de $X^2_t = 3.84 < X^2_C = 14.90$

Por consiguiente se acepta la hipótesis alterna.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al aplicar los instrumentos de recolección de información al personal de Industrias Catedral, se evidencio, que, aun cuando existen algunas restricciones informáticas, no existen políticas bien definidas de uso y confidencialidad de los recursos informáticos.

Las pocas restricciones informáticas existentes no son conocidas por todos los usuarios. La falta de una cultura informática en los usuarios ha puesto en eminente riesgo la información crítica de la empresa en varias ocasiones

Al no existir un criterio de valoración de los activos informáticos de Industrias Catedral, ha dificultado determinar los activos de mayor importancia para la empresa, siendo esto un limitante al momento de establecer el impacto que ocasionaría la perdida de un activo informático.

Recomendaciones

Es necesario realizar un Estudio de Análisis de Riesgos Informáticos en Industrias Catedral. Este estudio permitirá establecer criterios de valoración a los activos de acuerdo a parámetros, esto en dependencia de la metodología que se utilice, determinando así los activos de mayor importancia para la empresa. A la vez esto ayudara a definir los riesgos a los cuales están expuestos los activos, estableciendo el grado de incidencia que estos tendrían al materializarse.

El Estudio de Análisis de Riesgos Informáticos ayudara a determinar los salvaguardas necesarios para disminuir o eliminar en su totalidad los riesgos informáticos existentes en Industrias Catedral

Es importante entender la importancia de diseñar e implementar los procesos, mecanismos y métricas necesarias que permitan proteger los activos informáticos de la empresa, pues de estos depende el correcto funcionamiento de la misma.

CAPITULO VI
LA PROPUESTA

Datos Informativos

Nombre de la Institución:	Industrias Catedral S.A.
Provincia:	Tungurahua
Parroquia:	San Vicente de Atahualpa
Dirección:	Av. Rodrigo Pachano y Batallón Montecristi
Teléfono:	2854820 – 2854789
Jornadas:	Matutina Vespertina Nocturna
Beneficiarios:	Usuarios del Sistema Informático
Tiempo Estimado:	Durante 1 año

Equipo Técnico Responsable:

- ✓ Departamento de Sistemas.

Antecedentes de la Propuesta

Ante el esquema de globalización que las tecnologías de la información han originado, principalmente por el uso masivo y universal de la Internet y sus tecnologías durante los últimos años, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crakers, etc., es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país la mayoría de organizaciones se han visto sujetas a los ataques en sus instalaciones, tanto desde el interior como del exterior.
Nuestra carencia de personal capacitado en seguridad informática, la escasa concientización, la falta de visión y las limitantes económicas han retrasado el plan rector de seguridad informática que se requiere en nuestro medio.

Justificación

Los ataques informáticos a las organizaciones en muchos de los países se han convertido en una cuestión de seguridad nacional. Continuamente aparecen nuevos delitos informáticos que ponen en riesgo los activos de las organizaciones.
La mayor parte de ataques informáticos se da desde dentro de la organización por parte de los usuarios internos, en unas ocasiones sin mala intención, si no más bien por falta de conocimientos en materia de seguridad.
De ahí que realizar un Estudio de análisis de Riesgos en Industrias Catedral, nos permitirá determinar las posibles amenazas a los cuales están expuestos, lo cual, al materializarse afectaría el correcto funcionamiento de la empresa. En base a este estudio se podrá definir Políticas de Seguridad Informática que con base en la política institucional proteja los activos de la organización.
La falta de Políticas de Seguridad Informática bien definidas, deja a la información crítica de una empresa, a la deriva de cualquier persona inescrupulosa

Requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

Así pues, ante este panorama surge el siguiente proyecto de Analisis de Riesgos Informaticos en Industrias Catedral como la herramienta que permitirá establecer ejes de proyección que en materia de seguridad, la organización requiere, a través de Políticas de Seguridad Informática bien definidas.

OBJETIVOS

GENERAL

Realizar un estudio de análisis de riesgos que permitan determinar las **políticas de seguridad y** los **riesgos informáticos** en los activos de Industrias Catedral S.A.

ESPECIFICOS

- Establecer los activos mas importantes de la empresa y los riesgos informaticos a los cuales están expuestos.

- Determinar el impacto que los riesgos causarían al materializarce sobre un activo.

- Elaborar un Manual de Políticas de Seguridad para reducir los riesgos en los activos informáticos de Industrias Catedral.

Análisis de Factibilidad

Ante los eminentes ataques informáticos, las organizaciones demandan de protección a los activos informáticos.
Las Políticas de Seguridad Informática emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permitan a Industrias Catedral cumplir con su misión, estas a su vez permitirán tener confiabilidad, disponibilidad e integridad en los activos informáticos de la organización.

Tecnológica

El avance tecnológico ha sido de gran ayuda a las organizaciones en varios ámbitos, como: sistematización de procesos, elaboración de un producto, entre otros.
Industrias Catedral, consciente de este avance y siendo una empresa a la vanguardia de la tecnología, cuenta con un Departamento Informático, en el cual colaboran dos

Ingenieros en Sistemas que están a cargo del correcto funcionamiento del mismo. En el área administrativa existe equipos tecnológicos actualizados para el procesamiento de información, permitiendo así obtener resultados prontos y oportunos para la toma de decisiones a nivel gerencial. En el área de producción también posee equipos de cómputo que comandan la producción del producto. También cuenta con software creado en la empresa, el mismo que se adapta a las necesidades de la organización
No obstante, si bien este avance tecnológico ha sido de gran ayuda, esto ha implicado que sin los debidos controles se ponga en riesgo a la información.

Económica Financiera

Industrias Catedral cuenta con un presupuesto para nuevos proyectos del área de Sistemas. Este financiamiento consta en el Presupuesto Anual Industrias Catedral, en el mismo se contempla entre otros: Capacitación al personal, adquisición de nuevos equipos, implementación de nuevos proyectos de mejora propuestos por los responsables del área informática.

Fundamentación

Norma ISO/IEC 17799

La Norma ISO/IEC 17799 establece dominios de control que cubren la Gestión de la Seguridad de la Información:

1. Políticas de Seguridad
2. Clasificación y control de activos: El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

3. Seguridad ligada al personal: Se orienta a proteger de las acciones del personal que opera con los activos de información. Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.
4. Seguridad física y del entorno: Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.
5. Gestión de comunicaciones y operaciones: Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
6. Control de accesos: Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.
7. Cumplimiento o conformidad de la legislación: La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Metodología

Metodología de Análisis de Riesgos MAGERIT

Activos Informáticos

[S]Servicios

Los servicios aparecen como activos de un análisis de riesgos y son:

- Servicios finales – Prestados por la organización a terceros

- Servicios contratados a terceros – A otra organización que los proporciona por sus propios medios

[D] Datos/Información

Elementos de información que de forma singular o agrupada, representa el conocimiento de que se tiene algo.

Son activos abstractos que serán almacenados en equipos, soportes normalmente agrupados en bases de datos.

Están clasificados de la siguiente forma:

1. Datos Vitales como por ejemplo datos de interés comercial – datos de gestión interna
2. Datos de carácter personal
3. Voz

1. Dícese de aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar aquellos que son imprescindibles para que la Organización supere una situación de emergencia, aquellos que permiten desempeñar o reconstruir las misiones críticas, aquellos sustancian la naturaleza legal o los derechos financieros de la Organización o sus usuarios.

2. Dícese de aquellos que tienen valor para la prestación de los servicios propios de la organización.

3. Dícese de cualquier información concerniente a personas físicas identificadas o identificables.

Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

[SW] Aplicaciones (software)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

En este apartado no interviene el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

[prp] desarrollo propio (in house)

[sub] desarrollo a medida (subcontratado)

[std] estándar (off the shelf)

[HW] Equipos informáticos (hardware)

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[host] grandes equipos (1)

[mid] equipos medios (2)

[pc] informática personal (3)

[mobile] informática móvil (4)

[pda] agendas electrónicas[easy] fácilmente reemplazable (5)

[data] que almacena datos (6)

[peripheral] periféricos

1. Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.
2. Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.
3. Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.
4. Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.
5. Son aquellos equipos que, en caso de avería temporal o definitiva pueden ser reemplazados pronta y económicamente.
6. Son aquellos equipos en los que los datos permanecen largo tiempo. En particular, se clasificarán de este tipo aquellos equipos que disponen de los datos localmente, a diferencia de aquellos que sólo manejan datos en tránsito.
7. Dícese de impresoras y servidores de impresión.
8. Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.

[COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[PSTN] red telefónica

[ISDN] rdsi (red digital)

[X25] X25 (red de datos)

[ADSL] ADSL

[pp] punto a punto

[radio] red inalámbrica

[sat] por satélite

[LAN] red local

[MAN] red metropolitana

[Internet] Internet

[vpn] red privada virtual

[SI] Soportes de información

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[electronic] electrónicos

[disk] discos

[san] almacenamiento en red

[disquette] disquetes

[cd] cdrom (CD-ROM)

[usb] dispositivos USB

[dvd] DVD

[tape] cinta magnética

[mc] tarjetas de memoria

[ic] tarjetas inteligentes

[non_electronic] no electrónicos

[printed] material impreso

[tape] cinta de papel

[film] microfilm

[cards] tarjetas perforadas

[L] Instalaciones

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

[site] emplazamiento

[building] edificio

[local] local

[mobile] plataformas móviles

[car] vehículo terrestre: coche, camión, etc

.

[plane] vehículo aéreo: avión, etc.

[ship] vehículo marítimo: buque, lancha, etc.

[shelter] contenedores

[channel] canalización

Datos de carácter personal

La clasificación de los datos de carácter personal depende de la legislación aplicable en cada lugar y circunstancia. En el caso de la legislación española, se ajusta a los dispuesto en

• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
(B.O.E. Nº 298, de 14 de diciembre de 1999)

• Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (B.O.E.Nº 151, de 25 de junio de 1999)
Esta legislación establece los siguientes criterios:

Nivel básico

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. LOPD artículo 3. RD artículo 4.1.

Nivel medio

Datos de carácter personal relativos a la comisión de infracciones administrativas o penales, Hacienda Pública o servicios financieros. RD artículos 4.2 y 4.4.

Nivel alto

Datos de carácter personal relativos a ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales sin consentimiento de las personas afectadas. RD artículo 4.3.

Criterio de Valoración en la Metodología de Análisis de Riesgos MAGERIT

Frecuentemente la valoración de un activo es cualitativa. Para valorar un activo utilizando la metodología MAGERIT se toma en consideración las siguientes situaciones:

Valor	Criterio
10 muy alto daño	Muy grave a la organización
7-9 alto daño	Grave a la organización
4-6 medio daño	Importante a la organización
1-3 bajo daño	Menor a la organización
0 despreciable	Irrelevante a efectos prácticos

Una vez establecido el rango se debe definir el área a la que causaría daño

Nivel 0	
	No afectaría a la seguridad de las personas
	Sería causa de inconveniencias mínimas a las partes afectadas
	Supondría pérdidas económicas mínimas
	No supondría daño a la reputación
Nivel 1	
	Pudiera causar la interrupción de actividades propias de la organización
	Administración y Gestión: pudiera impedir la operación efectiva de la organización
	Pudiera causar una pérdida menor de la confianza dentro de la organización
	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (Ámbito Local)
	Pudiera causar algún daño menor a misiones importantes de inteligencia o información

	Intereses comerciales o económicos
	Información personal: pudiera causar molestias a un individuo
	Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley de regulación
Nivel 2	
	Probablemente cause una pérdida menor de la confianza dentro de la organización
	Intereses Comerciales o económicos
	Información personal: pudiera causar molestias a un individuo
	Información personal: pudiera quebrantar de forma leve leyes o regulaciones
	Seguridad de las personas: pudiera causar daño menor a varios individuos
	Información clasificada: sin clasificar
Nivel 3	
	Probablemente cause la interrupción de actividades propias de la organización
	Administración y Gestión: probablemente impediría la operación efectiva de una parte de la organización
	Probablemente afecte negativamente a las relaciones internas de la organización
	Probablemente merme la eficacia o seguridad de la misión operativa o logística (Ámbito Local)
	Probablemente cause algún daño menor a misiones importantes de inteligencia o información
	Intereses comerciales o económicos
	Información personal: probablemente afecte a un individuo
	Información personal: probablemente suponga el incumplimiento de una ley o regulación

	Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley de regulación
	Seguridad: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
	Seguridad de las personas: probablemente cause daños menores a un individuo
	Orden público: Causa de protestas puntuales
	Probablemente cause un impacto leve en las relaciones internacionales
	Información clasificada: difusión limitada
	RESTREINT UE
Nivel 4	
	Información Personal: probablemente afecte a un grupo de individuos
	Información personal: probablemente quebrante leyes o regulaciones
	Seguridad de las personas: probablemente cause daños menores a varios individuos
	Dificulte la investigación o facilite la comisión de delitos
	Información clasificada: difusión limitada
	RESTREINT UE
Nivel 5	
	Probablemente cause la interrupción de actividades propias de la organización con impacto en otras organizaciones
	Administración y Gestión: probablemente impediría la operación efectiva de más de una parte de la organización
	Probablemente sea causa de una cierta publicidad negativa

	Probablemente merme la eficacia o seguridad de la misión operativa o logística mas allá del ámbito local
	Probablemente dañe a misiones importantes de inteligencia o información
	Información personal: probablemente afecte gravemente a un individuo
	Información personal: probablemente quebrante seriamente leyes o regulaciones
	Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
	Probablemente tenga impacto en las relaciones internacionales
	Información clasificada: difusión limitada
Nivel 6	RESTREINT UE
	Información personal: probablemente afecte gravemente a un grupo de individuos
	información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo
	Orden público: probablemente cause manifestaciones o presiones significativas
	Información clasificada: difusión limitada
	RESTREINT UE
Nivel 7	
	Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
	Administración y gestión : probablemente impediría la operación efectiva de la organización

	Probablemente causaría una publicidad negativa generalizada
	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serio daños a misiones importantes de inteligencia o información
	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
	Seguridad : probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
	Probablemente cause un impacto significativo en las relaciones internacionales
	Información clasificada : confidencial
	confidential UE
Nivel 8	
	Seguridad de las personas: probablemente cause daño a la seguridad o libertad individual (por ejemplo es probable que llegue a amenazar la vida de uno o mas individuos)
	Impida la investigación de delitos graves o facilite su comisión
	Información clasificada : confidencial
	confidential UE
Nivel 9	
	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la organización con un serio impacto en otras organizaciones

	Administración y gestión : probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre
	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones
	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serios daños a misiones muy importantes de inteligencia o información
	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
	Seguridad de las personas: probablemente suponga la muerte de uno o mas individuos
	Orden público : Alteración seria del orden público
	Probablemente cause un serio impacto en las relaciones internacionales
	Información clasificada: reservado
	SECRET UE

Dimensiones de Valoración

La valoración se realiza a cada uno de los activos informáticos identificados en la organización basados en las dimensiones de:

Disponibilidad – Integridad – Confidencialidad - Autenticidad

Utilizando las escalas anteriores mencionadas

Amenazas

Se identificara algunas de las amenazas que afectarían a los activos informáticos

[N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Fuego	
Tipos de activos	**Dimensión**
[HW] equipos informáticos (hardware)	Disponibilidad
[COM] redes de comunicaciones	
[SI] soportes de información	
[AUX] equipamiento auxiliar	
[L] instalaciones	
Descripción: incendios - posibilidad de que el fuego acabe con recursos del sistema.	

Daños por agua	
Tipos de activos	**Dimensión**
[HW] equipos informáticos (hardware)	Disponibilidad
[COM] redes de comunicaciones	
[SI] soportes de información	
[AUX] equipamiento auxiliar	
[L] instalaciones	
Inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

Desastres Naturales	
Tipos de activos	**Dimensión**
[HW] equipos informáticos (hardware)	Disponibilidad
[COM] redes de comunicaciones	
[SI] soportes de información	
[AUX] equipamiento auxiliar	
[L] instalaciones	
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...	

Corte de Energía Eléctrica	
Tipos de activos	**Dimensión**
[HW] equipos informáticos (hardware)	Disponibilidad
[COM] redes de comunicaciones	
[SI] soportes de información (electrónicos)	
[AUX] equipamiento auxiliar	
Descripción : Cese de la alimentación de potencia	

Condición inadecuada de temperatura	
Tipos de activos	**Dimensión**
[HW] equipos informáticos (hardware)	Disponibilidad
[COM] redes de comunicaciones	
[SI] soportes de información	
[AUX] equipamiento auxiliar	
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...	

[E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Errores de los Usuarios	
Tipos de activos	**Dimensión**
[S] servicios	Integridad – Disponibilidad
[D] datos / información	
[SW] aplicaciones (software)	
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.	

Errores del Administrador	
Tipos de activos	**Dimensión**
[S] servicios	Integridad
[D] datos / información	Disponibilidad
[SW] aplicaciones (software)	Confidencialidad
[HW] equipos informáticos (hardware)	Autenticidad
[COM] redes de comunicaciones	
Descripción: equivocaciones de personas con responsabilidades de instalación y operación	

Difusión de Software Dañino	
Tipos de activos	**Dimensión**
[SW] aplicaciones (software)	Disponibilidad
Propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. equivocaciones de personas con responsabilidades de instalación y operación	

Alteración de la información	
Tipos de activos	**Dimensión**
Datos/Información	Integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

Modelado de las amenazas

Se denomina modelo de amenazas a la terminología utilizada para concretar la valoración de las amenazas: probabilidad y degradación.

Se puede utilizar varias maneras de plasmar las posibilidades que una amenaza tiene de ocurrir.

Potencial	**probabilidad**	**nivel**	**Facilidad**	**frecuencia** **intervalo previsto entre ocurrencias**
S pequeño	I improbable	B bajo	MD muy difícil	0.1 diez años
M medio	PP poco probable	M medio	D difícil	1 una vez al año
L grande	P probable	A alto	M medio	10 cada mes

XL extra grande	CS casi seguro	MA muy alto	F fácil	100 a diario

Para describir la degradación, se usa niveles de referencia:

Nivel	porcentaje
B – bajo	1%
M – medio	10%
A – alto	50%
MA – muy alto	90%
T – total	100%

Análisis mediante tablas del valor del Impacto

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que sin ser muy precisos, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas

Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

MB: muy bajo

B: Bajo

M: Medio

A: Alto

MA: Muy alto

Estimación del impacto

Se puede calcular el impacto en base a tablas de doble entrada

IMPACTO		DEGRADACION		
		1%	10%	100%
VALOR	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de estimación inmediata

Estimación del riesgo

Por otra parte se modela la frecuencia por medio de alguna escala sencilla:

MF: Muy frecuente (a diario)

F: Frecuente (mensual)

FN: Frecuencia normal (anual)

PF: Poco frecuente (cada varios años)

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

RIESGO		FRECUENCIA			
		PF	FN	F	MF
IMPACTO	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Aquellos activos que reciban una calificación de riesgo muy alto (MA) deberían ser objeto de atención inmediata, dándose como solución la planificación de salvaguardas Para implementar esta metodología se ha utilizado el Herramienta Pilar de Análisis de Riesgos Informáticos

Modelo Cualitativo

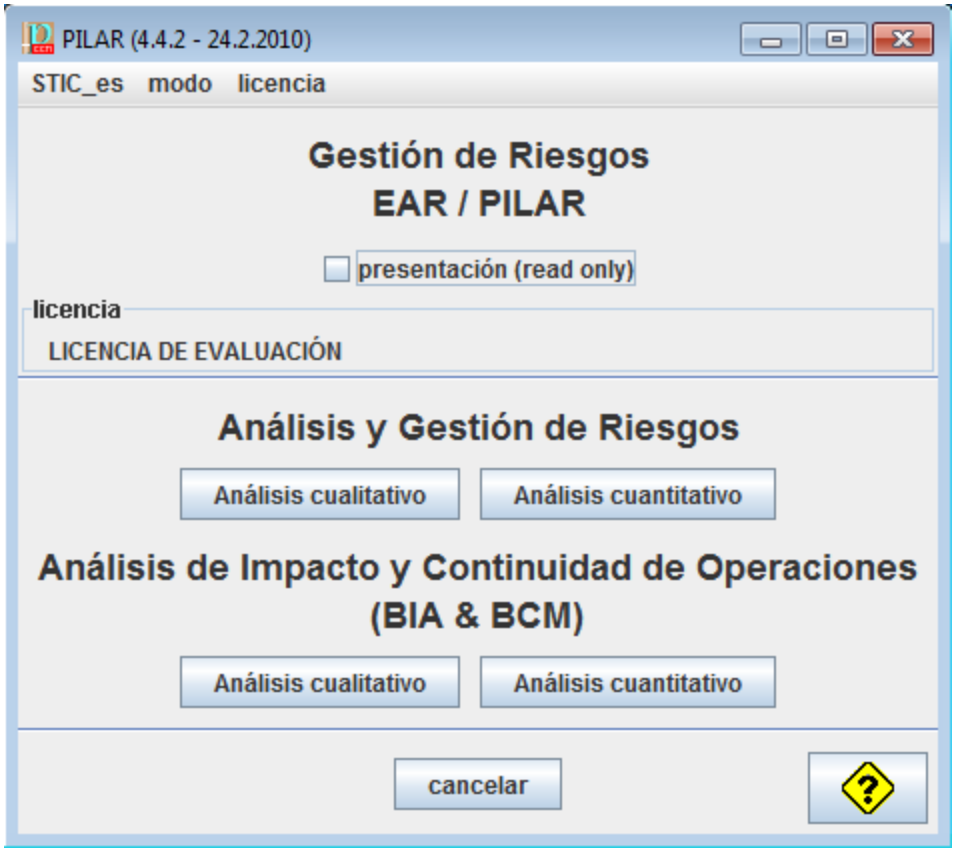
En un análisis de riesgo cualitativo se busca saber qué es lo que hay sin cuantificarlo con precisión, más allá de relativizar los elementos del modelo

Herramienta Pilar

La herramienta Pilar es una herramienta que ayudada de la metodología Magerit permite determinar los riesgos existentes en los activos informáticos de una organización. Además que basado en perfiles de seguridad da alternativas para eliminar o reducir este riesgo

Funcionamiento

Al iniciar esta herramienta nos muestra la siguiente pantalla

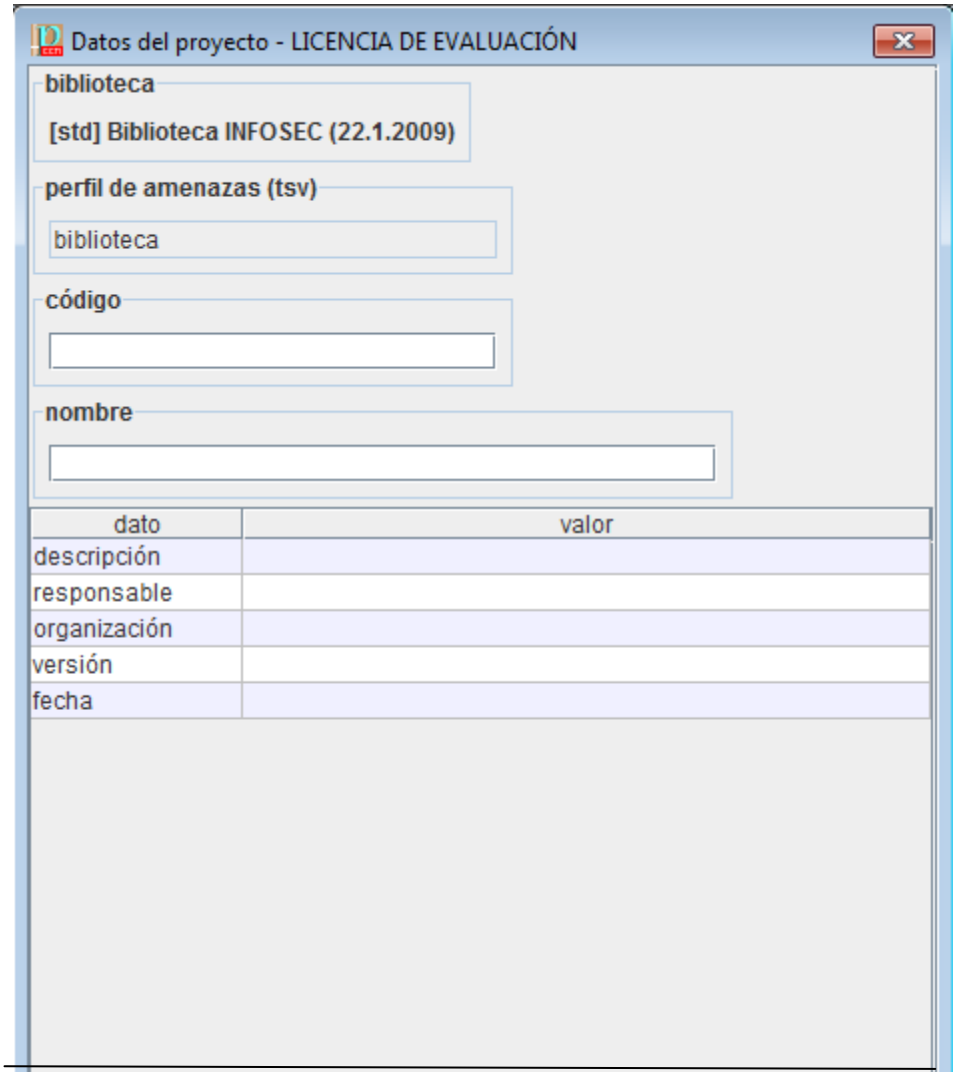


Para lo que nosotros necesitamos que es Análisis de Riesgos nos da dos alternativas:

Análisis Cualitativo

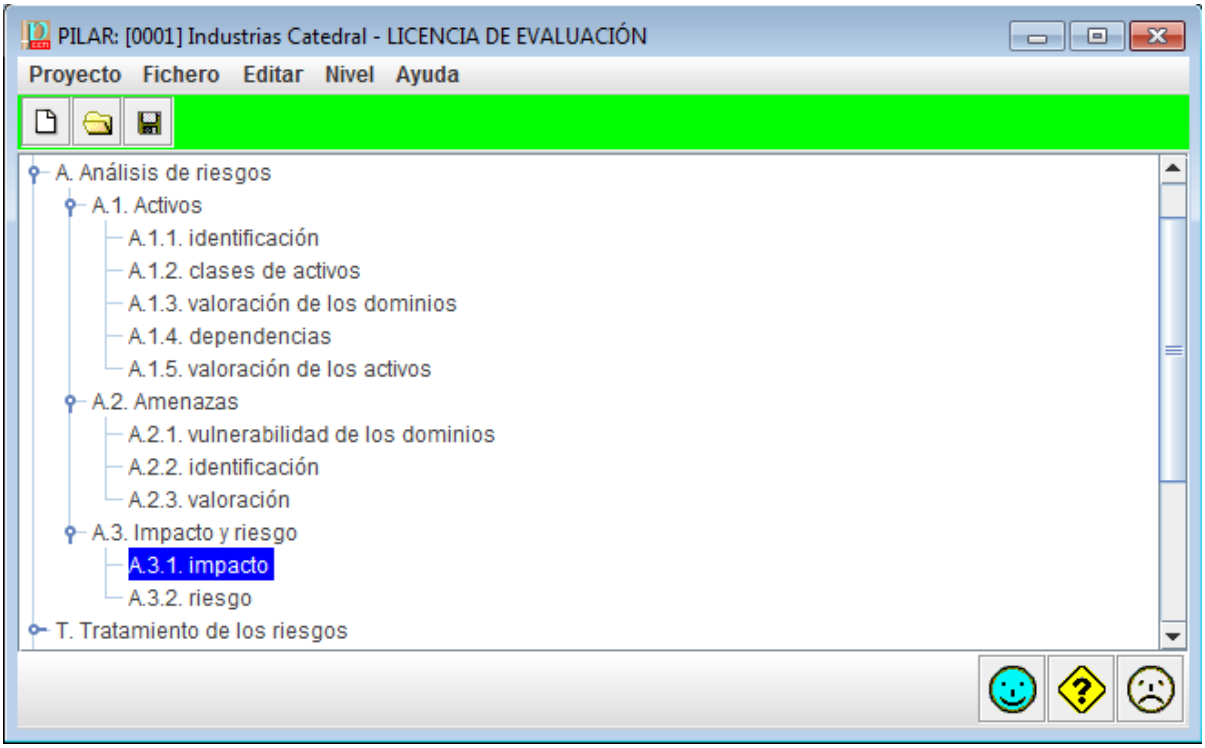
Análisis Cuantitativo

En este caso nos enfocaremos al análisis cualitativo. Damos click en Análisis cualitativo, mostrándonos la siguiente pantalla:



En esta pantalla se debe ingresar datos propios de l proyecto por ejemplo: un código 0001 y nombre Industrias Catedral

Posteriormente nos muestra la siguiente pantalla:



En esta pantalla tenemos un menú de opciones como:

Activos – En esta opción ingresaremos todos los activos informáticos de la empresa como también su valoración correspondiente

Amenazas – Se ingresa todas las posibles amenazas que podrían existir en la organización y su posible valor de degradación a l ser materializada

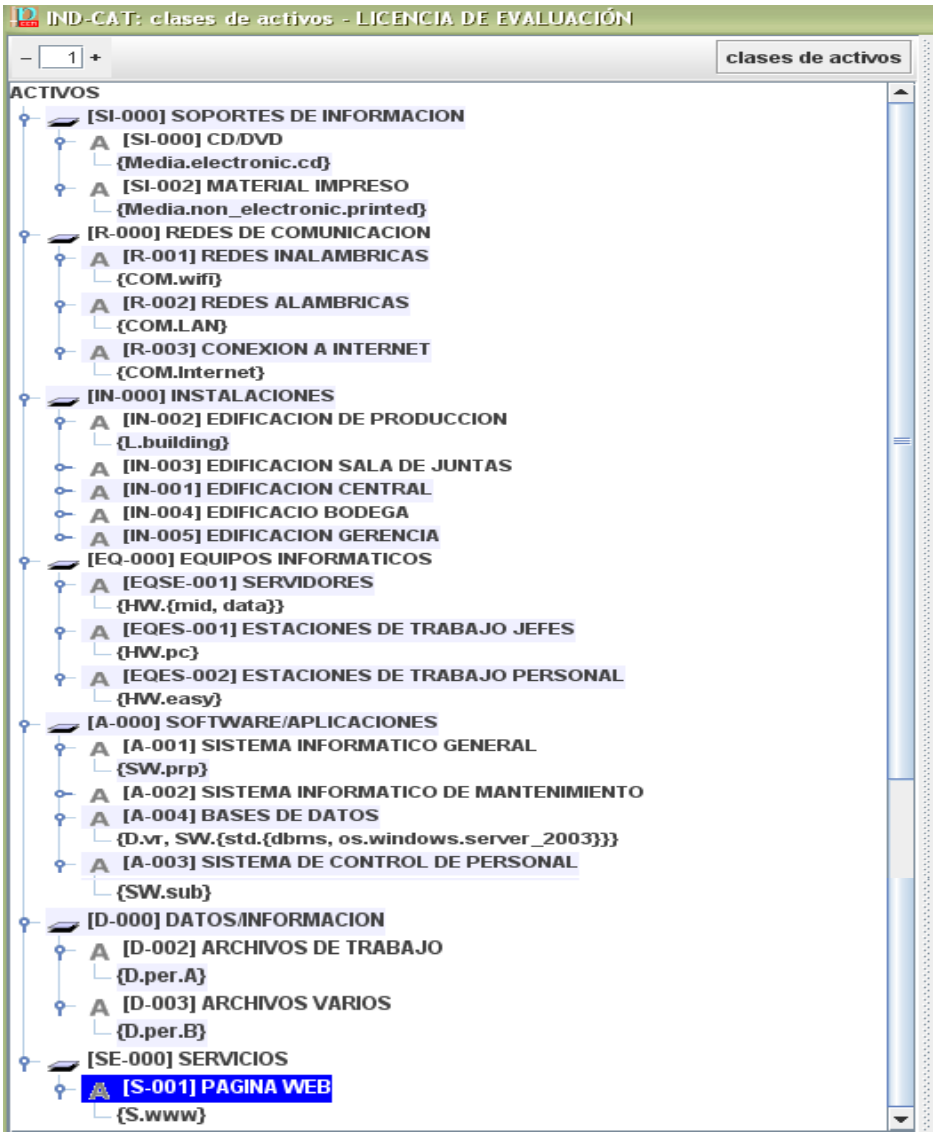
Impacto y Riesgo – Una vez ingresados los datos esta opción nos permitirá visualizar el impacto que una amenaza tendría al ser esta materializada

Modelo Operativo

Análisis De Riesgos Informáticos en Industrias Catedral

Para determinar los riesgos informáticos existentes en Industrias Catedral utilizaremos la herramienta PILAR versión de evaluación que hace uso de la Metodología Magerit

1- En la herramienta Pilar ingresamos los activos con la clasificación propia de la empresa. En este caso la clasificación de los activos es:



2- Una vez ingresados los activos con la debida clasificación damos un valor a los activos. Para lo cual utilizamos los siguiente criterios de valoración de los activos informáticos

Soportes de Información

Activo : CD/DVD

Impresiones

Dimensión: Disponibilidad

Nivel 7	
	Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
X	Administración y gestión : probablemente impediría la operación efectiva de la organización
	Probablemente causaría una publicidad negativa generalizada
X	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serio daños a misiones importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
	Seguridad : probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
	Probablemente cause un impacto significativo en las relaciones internacionales
	Información clasificada : confidencial
	confidential UE

Redes de Comunicación

Activo : Redes Inalámbricas

Dimensión: Disponibilidad

Nivel 1	
X	Pudiera causar la interrupción de actividades propias de la organización
	Administración y Gestión: pudiera impedir la operación efectiva de la organización
X	Pudiera causar una pérdida menor de la confianza dentro de la organización
	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (Ámbito Local)
	Pudiera causar algún daño menor a misiones importantes de inteligencia o información
	Intereses comerciales o económicos
	Información personal: pudiera causar molestias a un individuo
	Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley de regulación

Activo : Redes Inalámbricas

Dimensión: Autenticidad

Nivel 9	
	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la organización con un serio impacto en otras organizaciones
X	Administración y gestión : probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre
	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones
	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serios daños a misiones muy importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
	Seguridad de las personas: probablemente suponga la muerte de uno o mas individuos
	Orden público : Alteración seria del orden público
	Probablemente cause un serio impacto en las relaciones internacionales
	Información clasificada: reservado
	SECRET UE

Activo : Redes alámbricas

Dimensión: Disponibilidad

Nivel 7	
	Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
X	Administración y gestión : probablemente impediría la operación efectiva de la organización
	Probablemente causaría una publicidad negativa generalizada
	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serio daños a misiones importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
	Seguridad : probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
	Probablemente cause un impacto significativo en las relaciones internacionales
	Información clasificada : confidencial
	confidential UE

Activo : Redes Alambricas

Dimensión: Autenticación

Nivel 9	
	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la organización con un serio impacto en otras organizaciones
X	Administración y gestión : probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre
	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones
	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serios daños a misiones muy importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
	Seguridad de las personas: probablemente suponga la muerte de uno o más individuos
	Orden público : Alteración sería del orden público
	Probablemente cause un serio impacto en las relaciones internacionales
	Información clasificada: reservado
	SECRET UE

Activo : Conexión a Internet

Dimensión: Disponibilidad

Nivel 7	
	Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
X	Administración y gestión : probablemente impediría la operación efectiva de la organización
	Probablemente causaría una publicidad negativa generalizada
	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serio daños a misiones importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
	Seguridad : probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
	Probablemente cause un impacto significativo en las relaciones internacionales
	Información clasificada : confidencial
	confidential UE

Activo : Conexión a Internet

Dimensión: Autenticidad

Nivel 3	
X	Probablemente cause la interrupción de actividades propias de la organización
X	Administración y Gestión: probablemente impediría la operación efectiva de una parte de la organización
	Probablemente afecte negativamente a las relaciones internas de la organización
	Probablemente merme la eficacia o seguridad de la misión operativa o logística (Ámbito Local)
	Probablemente cause algún daño menor a misiones importantes de inteligencia o información
X	Intereses comerciales o económicos
	Información personal: probablemente afecte a un individuo
	Información personal: probablemente suponga el incumplimiento de una ley o regulación
	Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley de regulación
	Seguridad: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
	Seguridad de las personas: probablemente cause daños menores a un individuo
	Orden público: Causa de protestas puntuales
	Probablemente cause un impacto leve en las relaciones internacionales
	Información clasificada: difusión limitada
	RESTREINT UE

Instalaciones

Activo: Edificación Producción

Edificación Sala de Juntas

Edificación Bodega

Edificación Gerencia

Dimensión: Disponibilidad

Nivel 4	
X	Información Personal: probablemente afecte a un grupo de individuos
	Información personal: probablemente quebrante leyes o regulaciones
	Seguridad de las personas: probablemente cause daños menores a varios individuos
	Dificulte la investigación o facilite la comisión de delitos
	Información clasificada: difusión limitada
	RESTREINT UE

Activo: Edificación Central

Dimensión: Disponibilidad

Nivel 7	
	Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
X	Administración y gestión : probablemente impediría la operación efectiva de la organización
	Probablemente causaría una publicidad negativa generalizada
	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serio daños a misiones importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
	Seguridad : probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
	Probablemente cause un impacto significativo en las relaciones internacionales
	Información clasificada : confidencial
	confidential UE

Equipos Informáticos

Activo: Servidores

Dimensión: Disponibilidad, Autenticidad

Nivel 9	
	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la organización con un serio impacto en otras organizaciones
X	Administración y gestión : probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre
	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones
	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serios daños a misiones muy importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
	Seguridad de las personas: probablemente suponga la muerte de uno o más individuos
	Orden público : Alteración sería del orden público
	Probablemente cause un serio impacto en las relaciones internacionales
	Información clasificada: reservado
	SECRET UE

Activo : Estaciones de Trabajo de Jefes Departamentales

Dimensión: Disponibilidad

Nivel 7	
	Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
X	Administración y gestión : probablemente impediría la operación efectiva de la organización
	Probablemente causaría una publicidad negativa generalizada
	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	Probablemente cause serio daños a misiones importantes de inteligencia o información
X	Intereses comerciales o económicos
	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
	Seguridad : probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
	Probablemente cause un impacto significativo en las relaciones internacionales
	Información clasificada : confidencial
	confidential UE

Activo : Estaciones de Trabajo Jefes Departamentales

Dimensión: Autenticidad

Nivel 6	
X	Información personal: probablemente afecte gravemente a un grupo de individuos
	información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo
	Orden público: probablemente cause manifestaciones o presiones significativas
	Información clasificada: difusión limitada
	RESTREINT UE

Activo : Estaciones de Trabajo

Dimensión: Disponibilidad

Nivel 1	
X	Pudiera causar la interrupción de actividades propias de la organización
	Administración y Gestión: pudiera impedir la operación efectiva de la organización
	Pudiera causar una pérdida menor de la confianza dentro de la

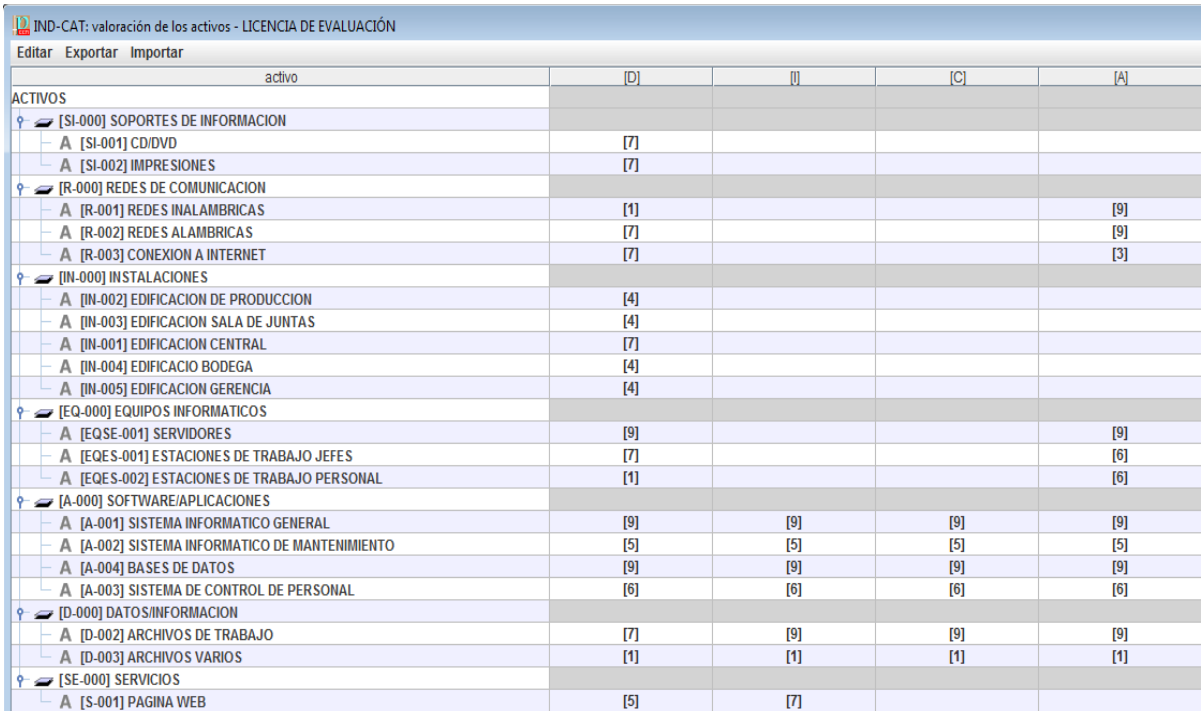
	organización
	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (Ámbito Local)
	Pudiera causar algún daño menor a misiones importantes de inteligencia o información
	Intereses comerciales o económicos
	Información personal: pudiera causar molestias a un individuo
	Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley de regulación

Activo : Estaciones de Trabajo

Dimensión: Autenticidad

Nivel 6	
X	Información personal: probablemente afecte gravemente a un grupo de individuos
	información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo
	Orden público: probablemente cause manifestaciones o presiones significativas
	Información clasificada: difusión limitada
	RESTREINT UE

Para establecer valores a los activos, se ha utilizado un cuestionario, el cual fue aplicado al Jefe de Sistemas de Industrias Catedral, quien en base a su experiencia en el área y ayudado de los criterios de valoración expuestos anteriormente, a determinado valores para cada activo. Estos valores fueron ingresados en la herramienta PILAR, como se muestra en la siguiente pantalla:



IND-CAT: valoración de los activos - LICENCIA DE EVALUACIÓN

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[SI-000] SOPORTES DE INFORMACION				
[SI-001] CD/DVD	[7]			
[SI-002] IMPRESIONES	[7]			
[R-000] REDES DE COMUNICACION				
[R-001] REDES INALAMBRICAS	[1]			[9]
[R-002] REDES ALAMBRICAS	[7]			[9]
[R-003] CONEXION A INTERNET	[7]			[3]
[IN-000] INSTALACIONES				
[IN-002] EDIFICACION DE PRODUCCION	[4]			
[IN-003] EDIFICACION SALA DE JUNTAS	[4]			
[IN-001] EDIFICACION CENTRAL	[7]			
[IN-004] EDIFICACIO BODEGA	[4]			
[IN-005] EDIFICACION GERENCIA	[4]			
[EQ-000] EQUIPOS INFORMATICOS				
[EQSE-001] SERVIDORES	[9]			[9]
[EQES-001] ESTACIONES DE TRABAJO JEFES	[7]			[6]
[EQES-002] ESTACIONES DE TRABAJO PERSONAL	[1]			[6]
[A-000] SOFTWARE/APLICACIONES				
[A-001] SISTEMA INFORMATICO GENERAL	[9]	[9]	[9]	[9]
[A-002] SISTEMA INFORMATICO DE MANTENIMIENTO	[5]	[5]	[5]	[5]
[A-004] BASES DE DATOS	[9]	[9]	[9]	[9]
[A-003] SISTEMA DE CONTROL DE PERSONAL	[6]	[6]	[6]	[6]
[D-000] DATOS/INFORMACION				
[D-002] ARCHIVOS DE TRABAJO	[7]	[9]	[9]	[9]
[D-003] ARCHIVOS VARIOS	[1]	[1]	[1]	[1]
[SE-000] SERVICIOS				
[S-001] PAGINA WEB	[5]	[7]		

La Figura 6.1, indica el Resumen de la Valoración de los Activos Informáticos

3- Una vez ingresados los activos e identificada su valoración es necesario determinar las posibles amenazas a los que podrían estar expuestos los activos informáticos para lo cual la herramienta Pilar en su base datos dispone de varios tipos de posibles amenazas. Siendo nosotros en base a nuestro criterio y a la situación propia de la empresa, quienes definimos las posibles amenazas para cada activo, como se muestra a cotinuacion:

SOPORTES DE INFORMACION

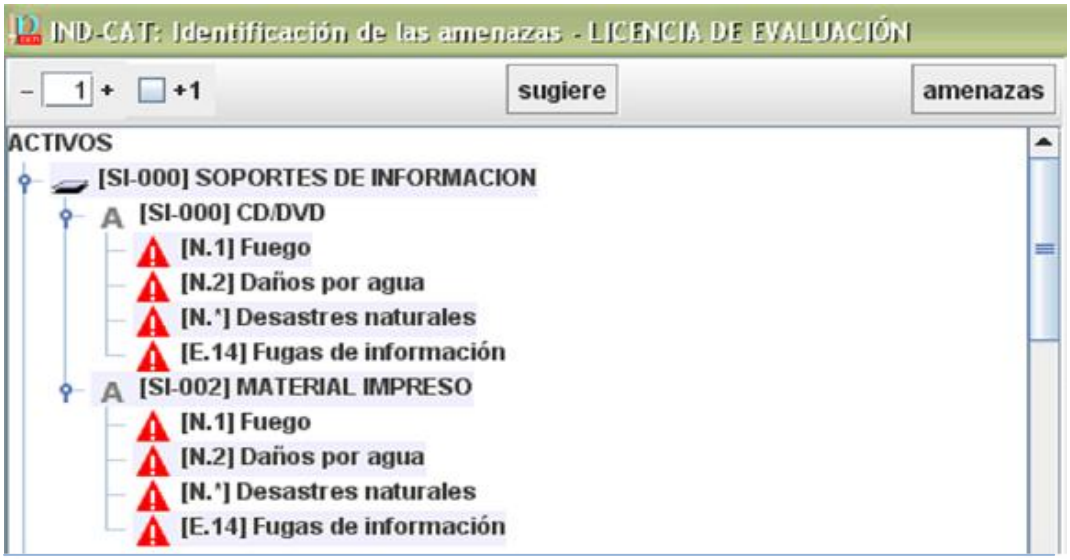


Figura 6.2: Posibles amenazas al Activo Soporte de Información

Una vez definidas las posibles amenazas es necesario determinar el valor de degradación que un activo tendría al ser materializada una amenaza. En este caso el porcentaje de degradación que tendría el activo soporte de información al materializarse cada una de las amenazas que identificamos. Este valor de degradación se debe dar en base a las dimensiones de valoración como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad

Es decir como afectaría la amenaza fuego a los soportes de información en cuanto a la disponibilidad. A continuación visualizamos los porcentajes de degradación dados a cada una de las amenazas del activo Soportes de Información

Porcentajes de degradación

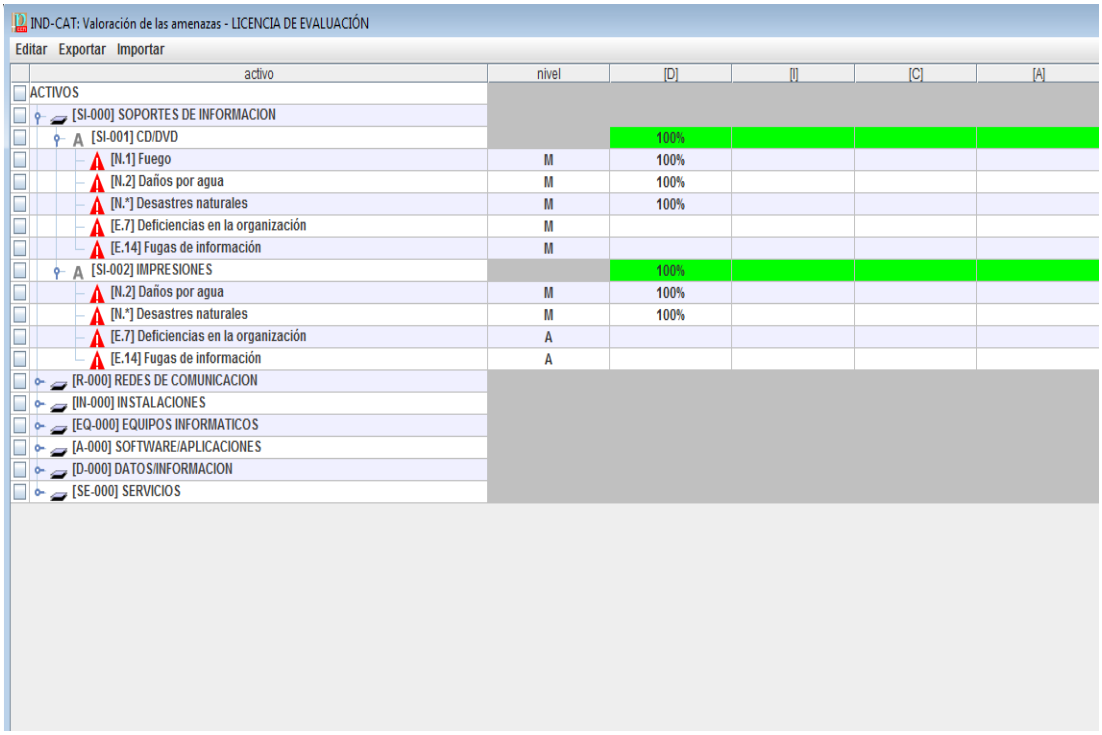


Figura 6.3 Porcentaje de degradación para las amenazas identificadas del activo Soportes de Información

Cabe mencionar que estos valores son dados en base a la experiencia y a la situación de la empresa. Valores que fueron tomados del cuestionario aplicado al Responsable de Sistemas

Lo anteriormente expuesto es aplicado a cada uno de los activos informáticos

REDES DE COMUNICACIÓN

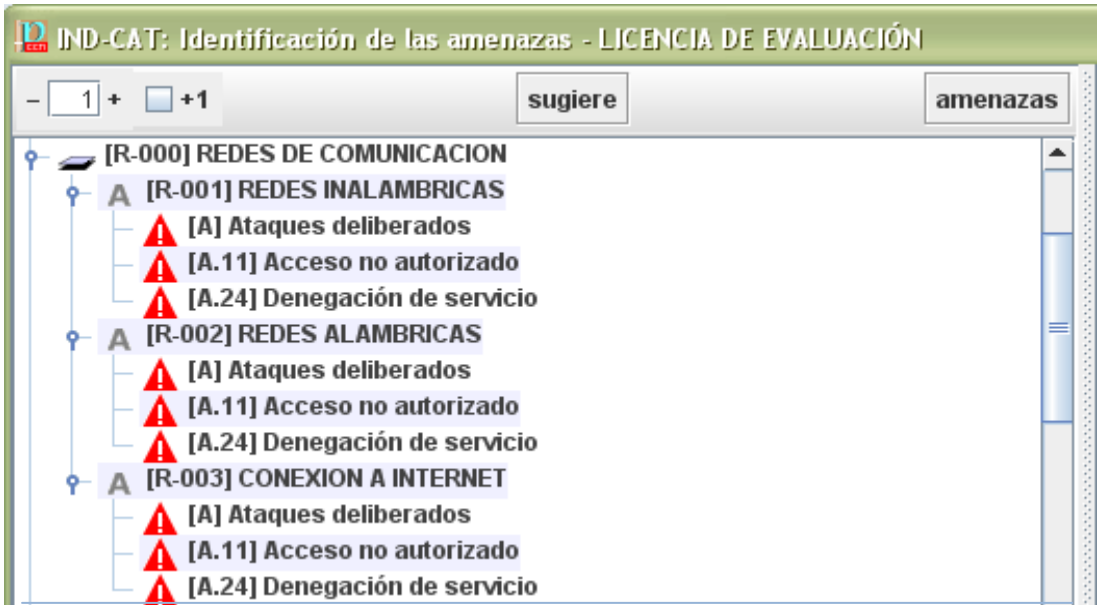
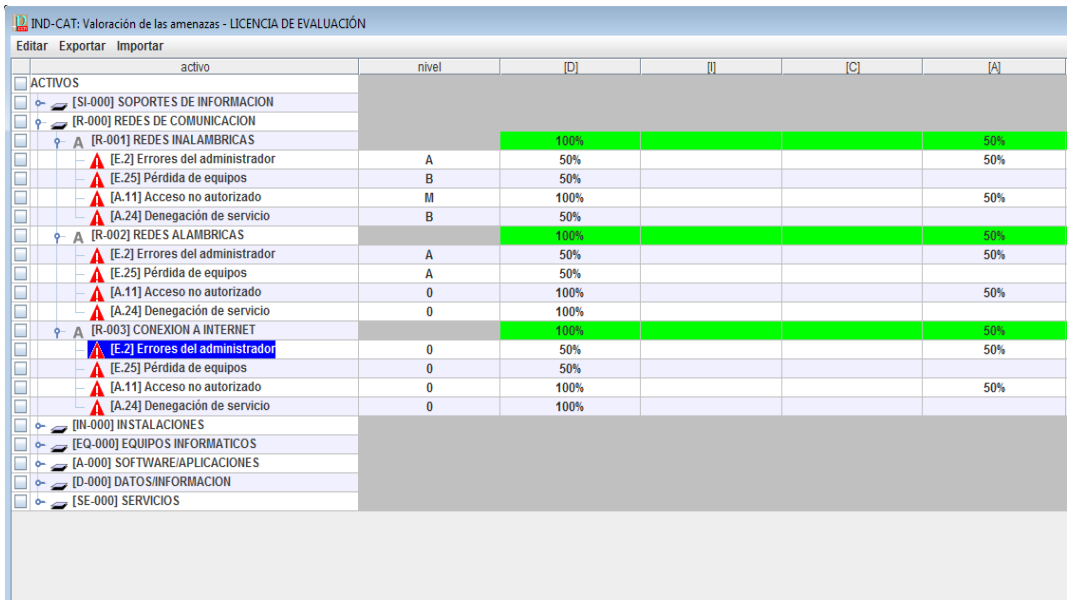


Figura 6.4 Posibles amenazas a las que podrían estar expuestos los activos Redes de Comunicación

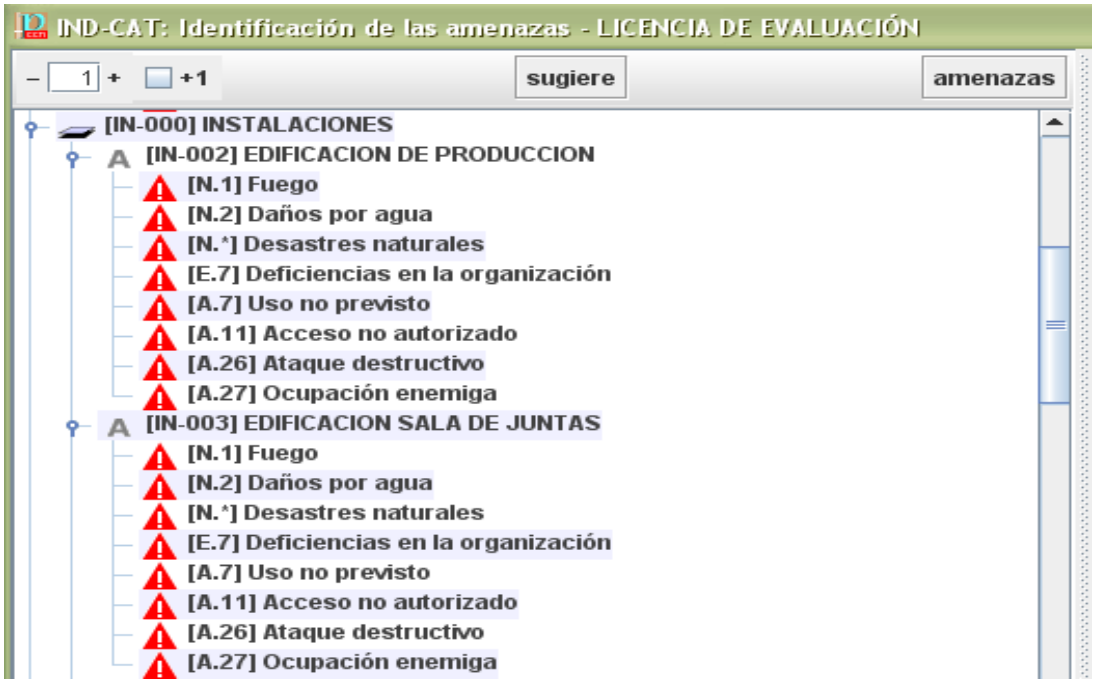
Porcentajes de degradación



activo	nivel	[D]	[I]	[C]	[A]
ACTIVOS					
[SI-000] SOPORTES DE INFORMACION					
[R-000] REDES DE COMUNICACION					
[R-001] REDES INALAMBRICAS		100%			50%
[E.2] Errores del administrador	A	50%			50%
[E.25] Pérdida de equipos	B	50%			
[A.11] Acceso no autorizado	M	100%			50%
[A.24] Denegación de servicio	B	50%			
[R-002] REDES ALAMBRICAS		100%			50%
[E.2] Errores del administrador	A	50%			50%
[E.25] Pérdida de equipos	A	50%			
[A.11] Acceso no autorizado	0	100%			50%
[A.24] Denegación de servicio	0	100%			
[R-003] CONEXION A INTERNET		100%			50%
[E.2] Errores del administrador	0	50%			50%
[E.25] Pérdida de equipos	0	50%			
[A.11] Acceso no autorizado	0	100%			50%
[A.24] Denegación de servicio	0	100%			
[IN-000] INSTALACIONES					
[EQ-000] EQUIPOS INFORMATICOS					
[A-000] SOFTWARE/APLICACIONES					
[D-000] DATOS/INFORMACION					
[SE-000] SERVICIOS					

Figura 6.5 nos indica el porcentaje de degradación para las amenazas identificadas del activo Redes de Comunicaciones

INSTALACIONES



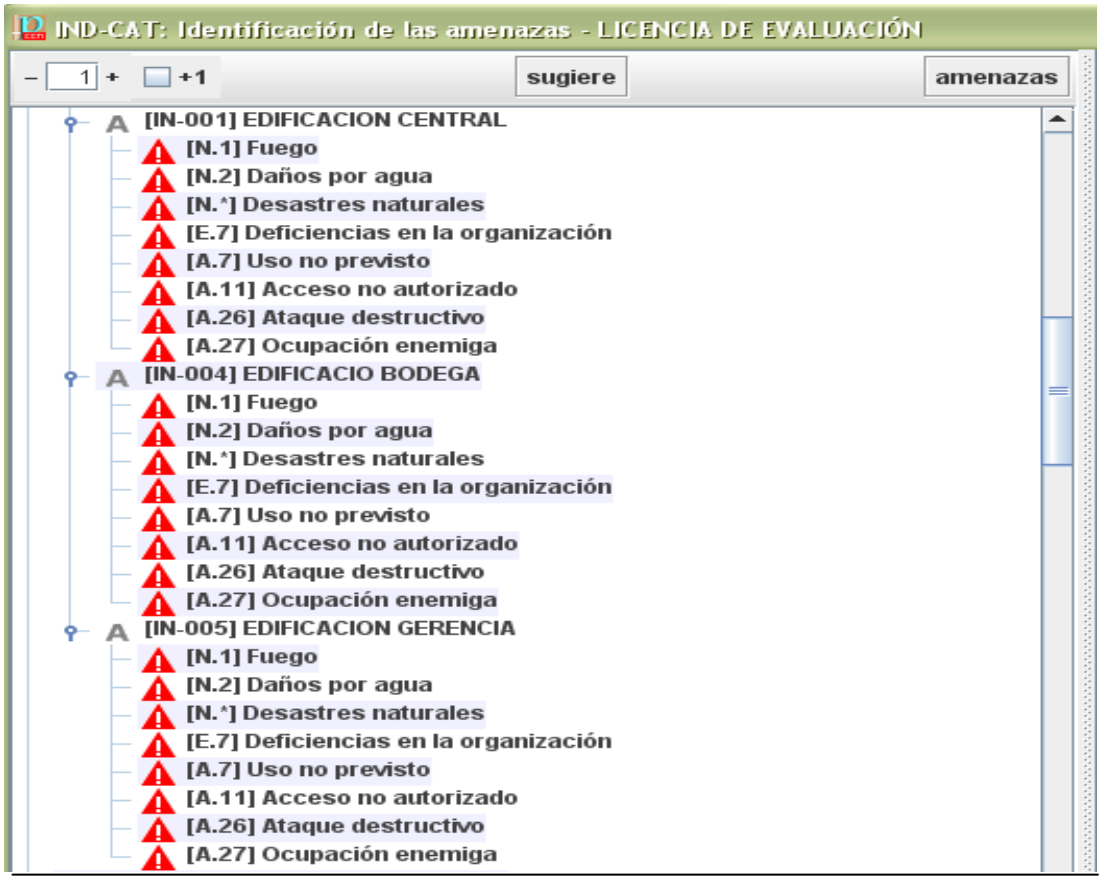
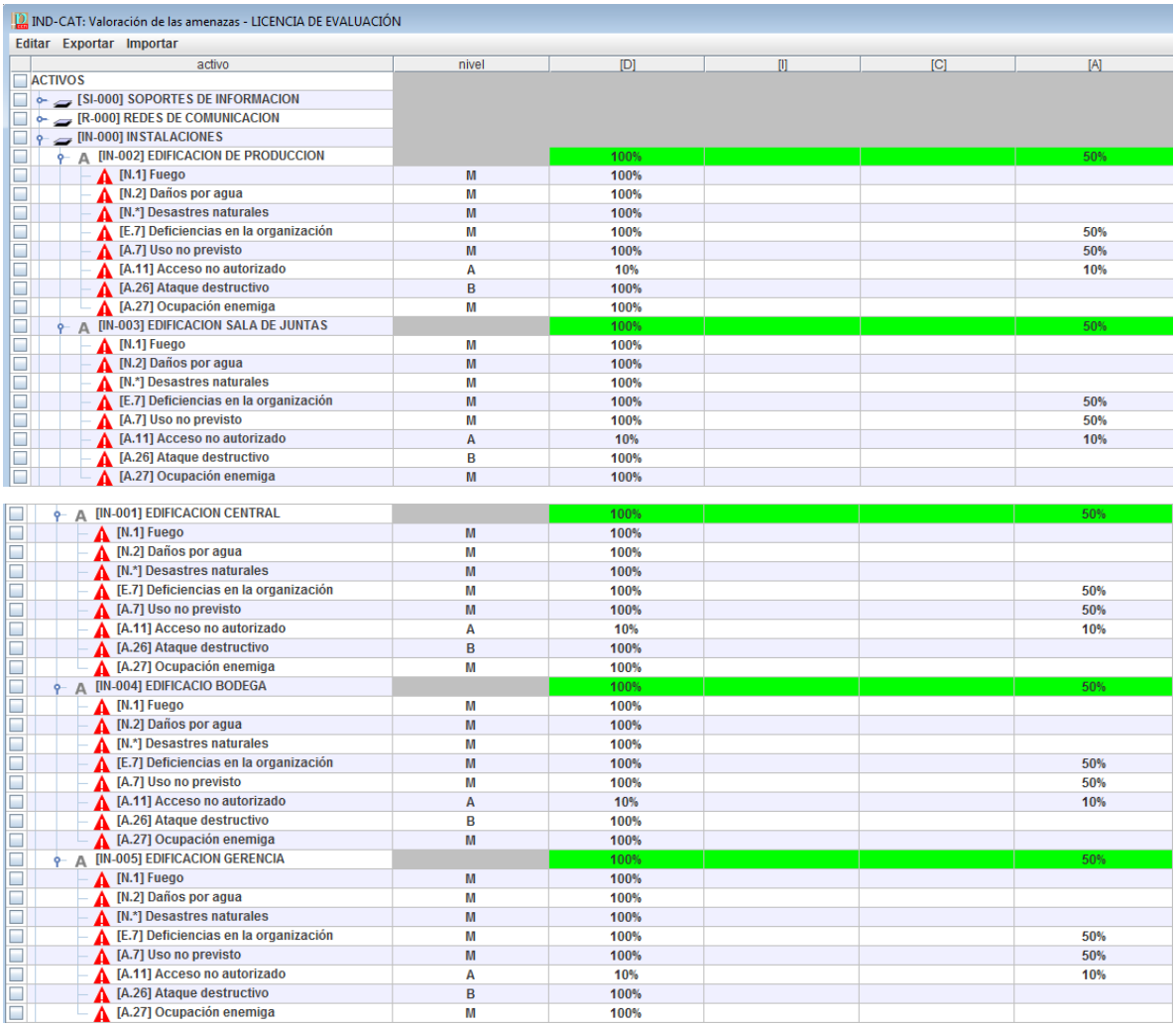


Figura 6.6 Indica las posibles amenazas a las que podrían estar expuestos los activos Instalaciones

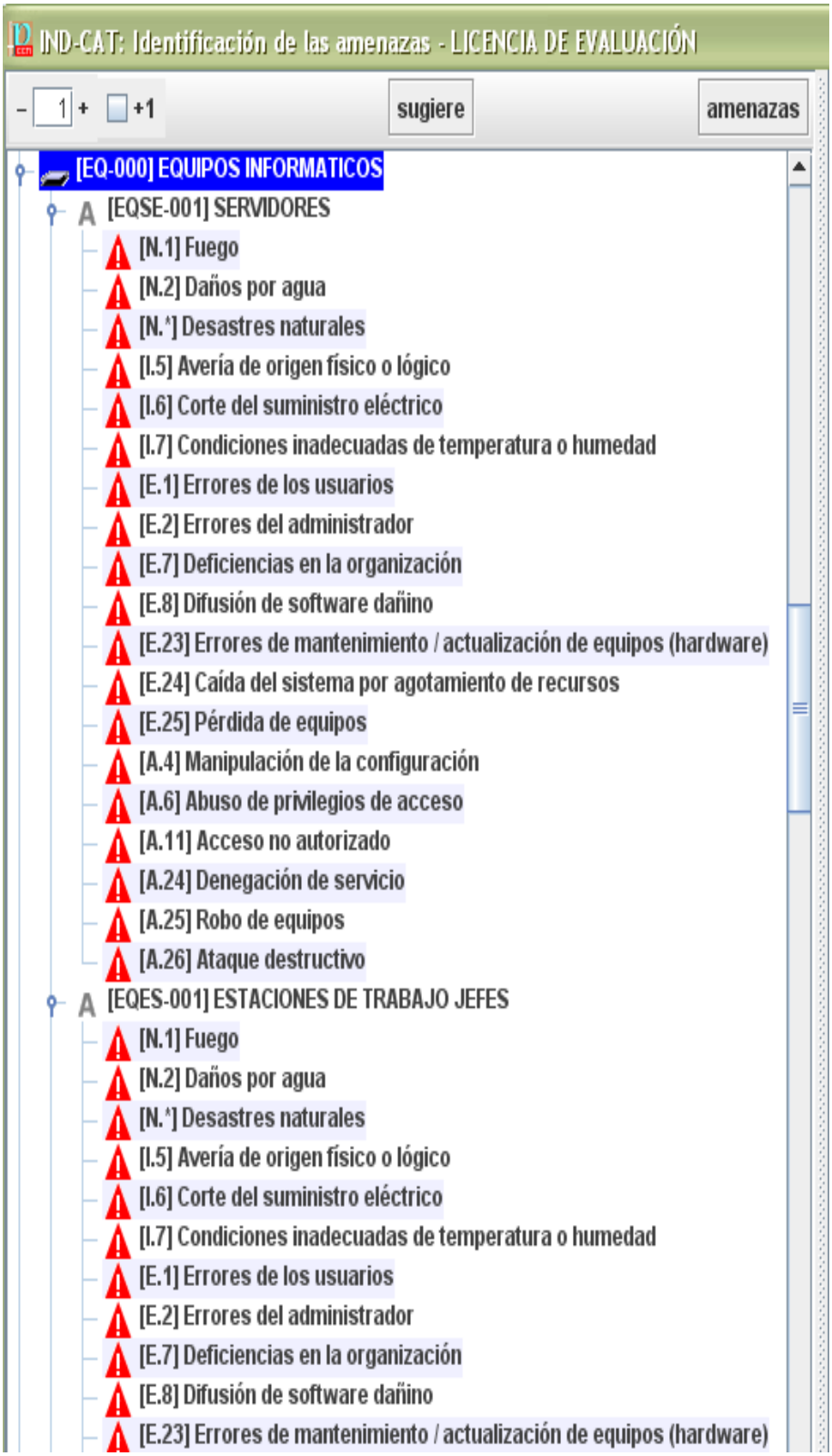
Porcentaje de degradación



activo	nivel	[D]	[I]	[C]	[A]
ACTIVOS					
[SI-000] SOPORTES DE INFORMACION					
[R-000] REDES DE COMUNICACION					
[IN-000] INSTALACIONES					
[IN-002] EDIFICACION DE PRODUCCION		100%			50%
[N.1] Fuego	M	100%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[E.7] Deficiencias en la organización	M	100%			50%
[A.7] Uso no previsto	M	100%			50%
[A.11] Acceso no autorizado	A	10%			10%
[A.26] Ataque destructivo	B	100%			
[A.27] Ocupación enemiga	M	100%			
[IN-003] EDIFICACION SALA DE JUNTAS		100%			50%
[N.1] Fuego	M	100%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[E.7] Deficiencias en la organización	M	100%			50%
[A.7] Uso no previsto	M	100%			50%
[A.11] Acceso no autorizado	A	10%			10%
[A.26] Ataque destructivo	B	100%			
[A.27] Ocupación enemiga	M	100%			
[IN-001] EDIFICACION CENTRAL		100%			50%
[N.1] Fuego	M	100%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[E.7] Deficiencias en la organización	M	100%			50%
[A.7] Uso no previsto	M	100%			50%
[A.11] Acceso no autorizado	A	10%			10%
[A.26] Ataque destructivo	B	100%			
[A.27] Ocupación enemiga	M	100%			
[IN-004] EDIFICACIO BODEGA		100%			50%
[N.1] Fuego	M	100%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[E.7] Deficiencias en la organización	M	100%			50%
[A.7] Uso no previsto	M	100%			50%
[A.11] Acceso no autorizado	A	10%			10%
[A.26] Ataque destructivo	B	100%			
[A.27] Ocupación enemiga	M	100%			
[IN-005] EDIFICACION GERENCIA		100%			50%
[N.1] Fuego	M	100%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[E.7] Deficiencias en la organización	M	100%			50%
[A.7] Uso no previsto	M	100%			50%
[A.11] Acceso no autorizado	A	10%			10%
[A.26] Ataque destructivo	B	100%			
[A.27] Ocupación enemiga	M	100%			

Figura 6.7 Indica el porcentaje de degradación para las amenazas identificadas del activo Instalaciones

Equipos Informáticos



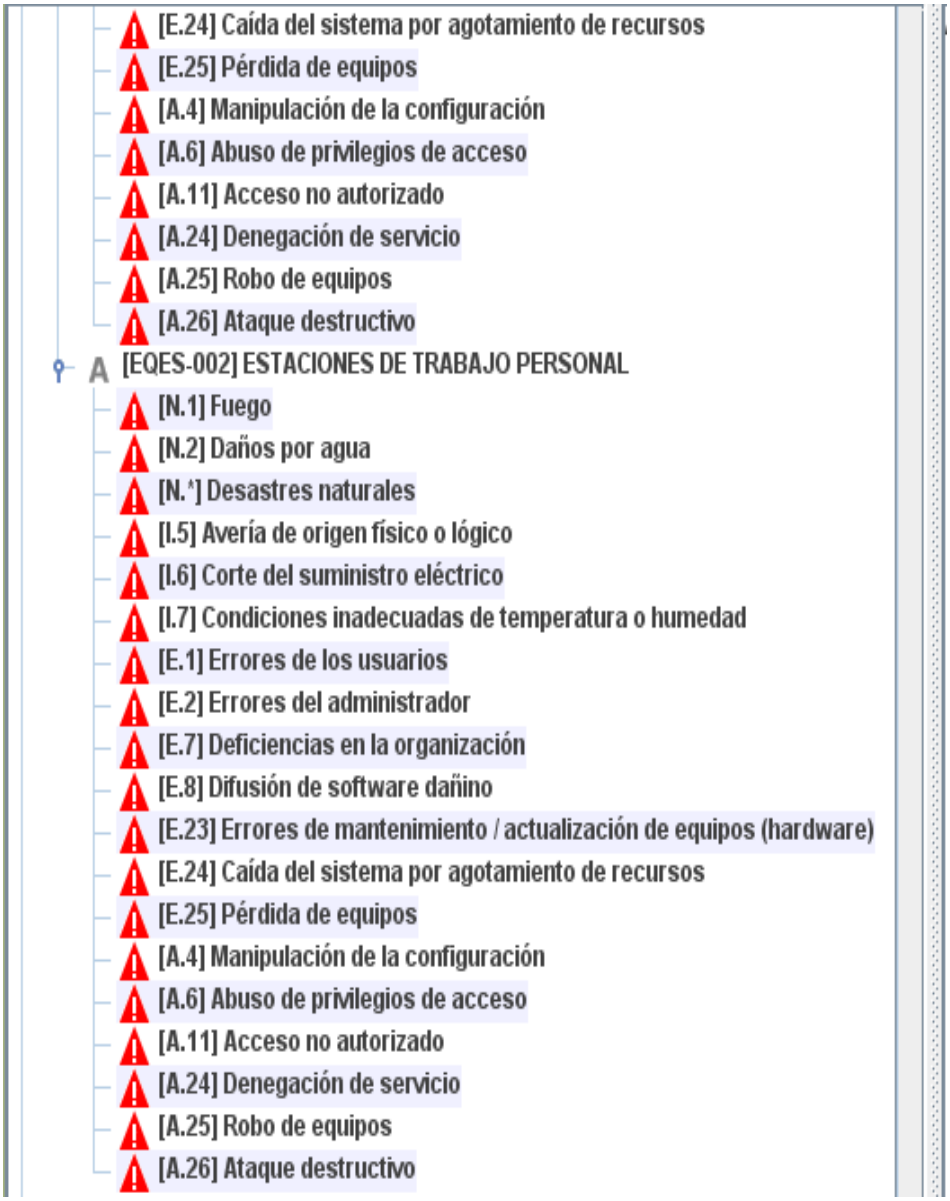


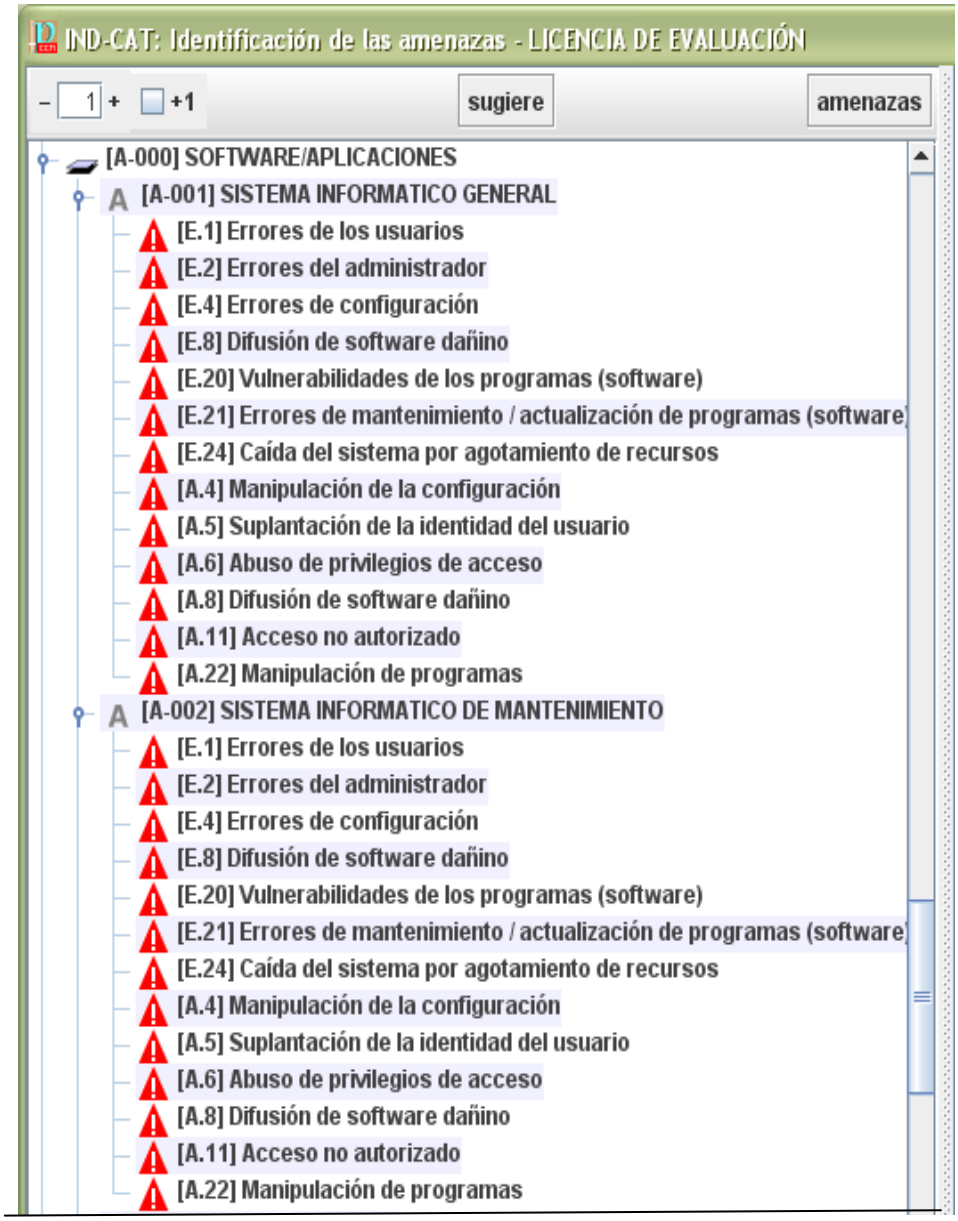
Figura 6.8 Indica las posibles amenazas a las que podrían estar expuestos los activos Equipos Informáticos

Porcentaje de Degradación

[EQ-000] EQUIPOS INFORMATICOS					
[EQSE-001] SERVIDORES		100%		100%	50%
[N.1] Fuego	B	100%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[I.5] Avería de origen físico o lógico	M	50%			
[I.6] Corte del suministro eléctrico	M	100%			
[I.7] Condiciones inadecuadas de temperatura	A	100%			
[E.2] Errores del administrador	M	50%		10%	10%
[E.7] Deficiencias en la organización	M	100%		50%	10%
[E.23] Errores de mantenimiento / actualizació	M	10%			
[E.25] Pérdida de equipos	M	100%			
[A.4] Manipulación de la configuración	M	50%		10%	10%
[A.6] Abuso de privilegios de acceso	M			50%	
[A.11] Acceso no autorizado	A	100%		50%	50%
[A.25] Robo de equipos	M	100%		100%	
[A.26] Ataque destructivo	B	100%			
[EQES-001] ESTACIONES DE TRABAJO JEFES		100%		100%	50%
[N.1] Fuego	B	10%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[I.5] Avería de origen físico o lógico	M	50%			
[I.6] Corte del suministro eléctrico	M	100%			
[I.7] Condiciones inadecuadas de temperatura	A	100%			
[E.2] Errores del administrador	M	50%		10%	10%
[E.7] Deficiencias en la organización	M	100%		50%	10%
[E.23] Errores de mantenimiento / actualizació	M	10%			
[E.25] Pérdida de equipos	M	100%			
[A.4] Manipulación de la configuración	M	50%		10%	10%
[A.6] Abuso de privilegios de acceso	M			50%	
[A.11] Acceso no autorizado	A	100%		50%	50%
[A.25] Robo de equipos	M	100%		100%	
[A.26] Ataque destructivo	B	100%			
[EQES-002] ESTACIONES DE TRABAJO PERSONAL		100%		100%	50%
[N.1] Fuego	B	10%			
[N.2] Daños por agua	M	100%			
[N.*] Desastres naturales	M	100%			
[I.5] Avería de origen físico o lógico	M	50%			
[I.6] Corte del suministro eléctrico	M	100%			
[I.7] Condiciones inadecuadas de temperatura	A	100%			
[E.2] Errores del administrador	M	50%		10%	10%
[E.7] Deficiencias en la organización	M	100%		50%	10%
[E.23] Errores de mantenimiento / actualizació	M	10%			
[E.25] Pérdida de equipos	M	100%			
[A.4] Manipulación de la configuración	M	50%		10%	10%
[A.6] Abuso de privilegios de acceso	M			50%	
[A.11] Acceso no autorizado	A	100%		50%	50%
[A.25] Robo de equipos	M	100%		100%	
[A.26] Ataque destructivo	B	100%			

Figura 6.9 Indica el porcentaje de degradación para las amenazas identificadas del activo Equipo Informático

SOFTWARE / APLICACIONES



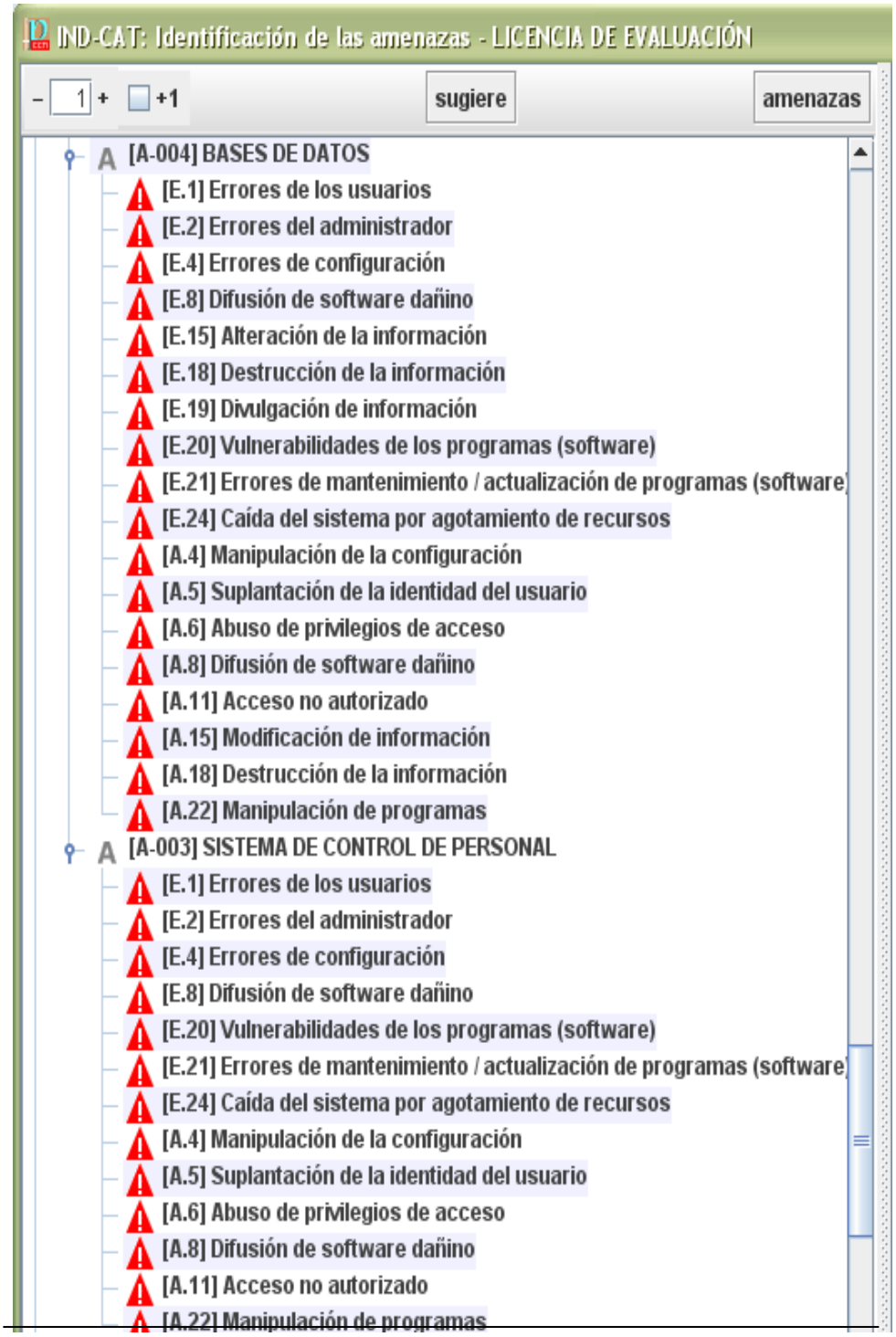


Figura 6.10 Indica las posibles amenazas a las que podrían estar expuestos los activos Software/Aplicaciones

Porcentaje de Degradación

[A-000] SOFTWARE/APLICACIONES					
[A-001] SISTEMA INFORMATICO GENERAL		100%		100%	100%
[E.1] Errores de los usuarios	A	1%		10%	
[E.2] Errores del administrador	M	100%		10%	50%
[E.4] Errores de configuración	M	50%		10%	50%
[E.7] Deficiencias en la organización	M	100%			
[A.4] Manipulación de la configuración	M	50%		50%	50%
[A.5] Suplantación de la identidad del usuario	A			100%	100%
[A.6] Abuso de privilegios de acceso	A			50%	100%
[A.8] Difusión de software dañino	A	50%		100%	100%
[A.11] Acceso no autorizado	A	100%		100%	100%
[A-002] SISTEMA INFORMATICO DE MANTENIMIEN		100%		100%	100%
[E.1] Errores de los usuarios	A	1%		10%	50%
[E.2] Errores del administrador	M	100%		10%	50%
[E.4] Errores de configuración	M	50%		10%	50%
[E.7] Deficiencias en la organización	M	100%			
[A.4] Manipulación de la configuración	M	50%		50%	50%
[A.5] Suplantación de la identidad del usuario	A			100%	100%
[A.6] Abuso de privilegios de acceso	A			50%	100%
[A.8] Difusión de software dañino	A	50%		100%	100%
[A.11] Acceso no autorizado	A	100%		100%	100%
[A-004] BASES DE DATOS		100%	50%	100%	100%
[E.1] Errores de los usuarios	A	10%	10%	100%	10%
[E.2] Errores del administrador	M	10%	10%	100%	100%
[E.4] Errores de configuración	M	50%	10%	50%	100%
[E.7] Deficiencias en la organización	M	100%	1%	100%	
[E.15] Alteración de la información	M				
[E.18] Destrucción de la información	M	100%			
[E.19] Divulgación de información	M			100%	
[A.4] Manipulación de la configuración	A	50%	10%	10%	100%
[A.5] Suplantación de la identidad del usuario	A		10%	50%	10%
[A.6] Abuso de privilegios de acceso	A			100%	50%
[A.8] Difusión de software dañino	A	50%		100%	50%
[A.11] Acceso no autorizado	A	100%	10%	100%	100%
[A.15] Modificación de información	M		50%	1%	1%
[A.18] Destrucción de la información	B	100%		1%	1%
[A-003] SISTEMA DE CONTROL DE PERSONAL		100%		100%	100%
[E.1] Errores de los usuarios	A	1%		10%	50%
[E.2] Errores del administrador	M	100%		10%	50%
[E.4] Errores de configuración	M	50%		10%	50%
[E.7] Deficiencias en la organización	M	100%			
[A.4] Manipulación de la configuración	M	50%		50%	50%
[A.5] Suplantación de la identidad del usuario	A			100%	100%
[A.6] Abuso de privilegios de acceso	A			50%	100%
[A.8] Difusión de software dañino	A	50%		100%	100%
[A.11] Acceso no autorizado	A			100%	100%

Figura 6.11 Indica el porcentaje de degradación para las amenazas identificadas del activo Software

DATOS / INFORMACION

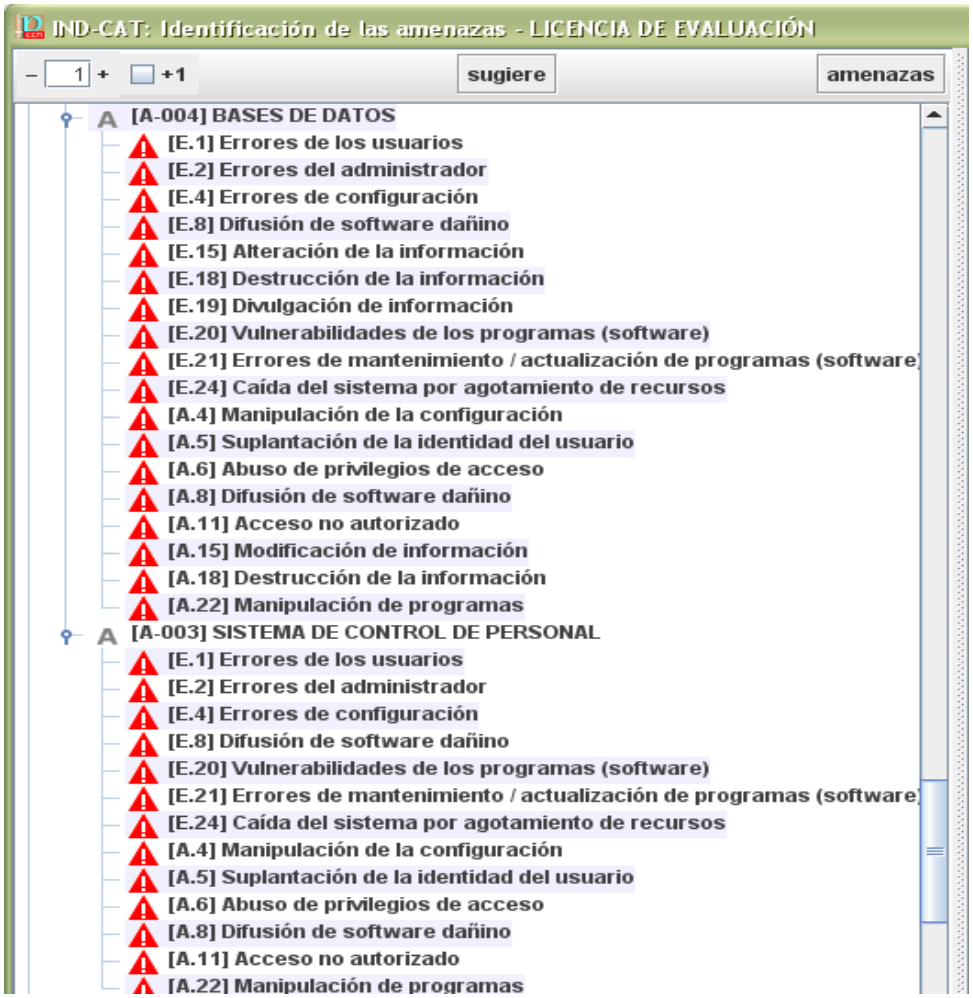


Figura N◦12 Indica las posibles amenazas a las que podrían estar expuestos los activos Datos/Información

Porcentaje de degradación

[D-000] DATOS/INFORMACION					
[D-002] ARCHIVOS DE TRABAJO		100%	50%	100%	50%
[E.1] Errores de los usuarios	A	10%	10%	10%	
[E.2] Errores del administrador	M	10%	10%	10%	10%
[E.4] Errores de configuración	M	50%	10%	10%	50%
[E.15] Alteración de la información	A		1%		
[E.16] Introducción de falsa información	MA		1%		
[E.18] Destrucción de la información	A	100%			
[E.19] Divulgación de información	M			50%	
[A.11] Acceso no autorizado	MA	100%	10%	50%	50%
[A.15] Modificación de información	A		50%		
[A.18] Destrucción de la información	A	100%	50%		
[A.19] Divulgación de información	A			100%	
[D-003] ARCHIVOS VARIOS		100%	50%	100%	50%
[E.1] Errores de los usuarios	A	10%	10%	10%	
[E.2] Errores del administrador	M	10%	10%	10%	10%
[E.4] Errores de configuración	M	50%	10%	10%	50%
[E.15] Alteración de la información	A		1%		
[E.16] Introducción de falsa información	MA		1%		
[E.18] Destrucción de la información	A	100%			
[E.19] Divulgación de información	M			50%	
[A.11] Acceso no autorizado	MA	100%	10%	50%	50%
[A.15] Modificación de información	A		50%		
[A.18] Destrucción de la información	A	100%	50%		
[A.19] Divulgación de información	A			100%	

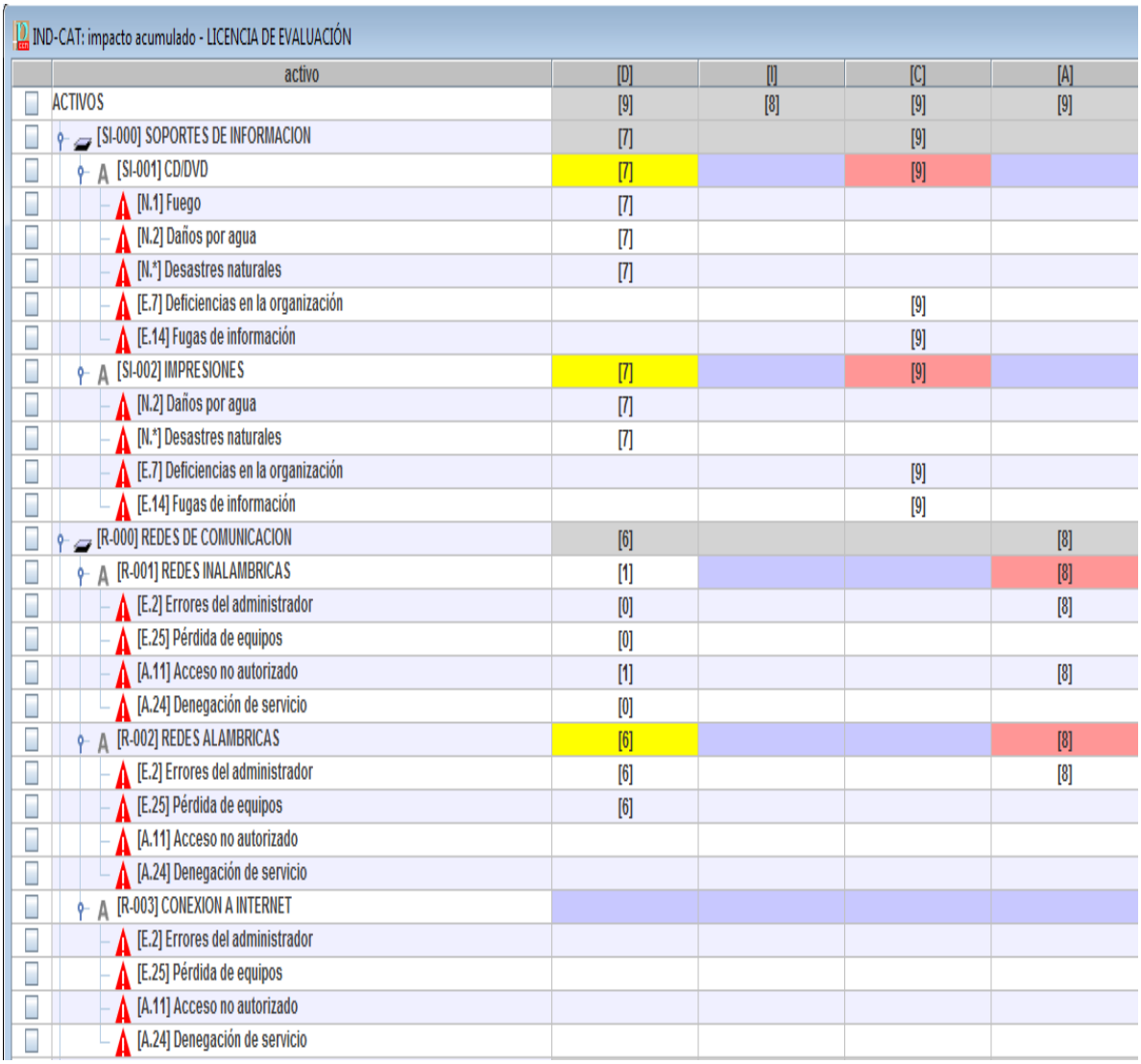
Figura 6.13 Indica el porcentaje de degradación para las amenazas identificadas del activo Datos/Información

SERVICIOS

[S-001] PAGINA WEB		100%			
[E.2] Errores del administrador	M	100%			
[E.4] Errores de configuración	M	100%			
[E.24] Caída del sistema por agotamiento de r	M	100%			
[A.4] Manipulación de la configuración	M	100%			
[A.24] Denegación de servicio	M	100%			

Figura 6.14 Indica el porcentaje de degradación para las amenazas identificadas del activo Servicios

Una vez ingresados los activos su valoración, las posibles amenazas con sus porcentajes de degradación, podemos obtener el siguiente cuadro que es un resumen del Impacto que las amenazas al ser materializadas tendrían sobre cada uno de los activos en cada dimensión de valoración



IND-CAT: impacto acumulado - LICENCIA DE EVALUACIÓN

activo	[D]	[I]	[C]	[A]
ACTIVOS	[9]	[8]	[9]	[9]
[SI-000] SOPORTES DE INFORMACION	[7]		[9]	
[SI-001] CD/DVD	[7]		[9]	
[N.1] Fuego	[7]			
[N.2] Daños por agua	[7]			
[N.*] Desastres naturales	[7]			
[E.7] Deficiencias en la organización			[9]	
[E.14] Fugas de información			[9]	
[SI-002] IMPRESIONES	[7]		[9]	
[N.2] Daños por agua	[7]			
[N.*] Desastres naturales	[7]			
[E.7] Deficiencias en la organización			[9]	
[E.14] Fugas de información			[9]	
[R-000] REDES DE COMUNICACION	[6]			[8]
[R-001] REDES INALAMBRICAS	[1]			[8]
[E.2] Errores del administrador	[0]			[8]
[E.25] Pérdida de equipos	[0]			
[A.11] Acceso no autorizado	[1]			[8]
[A.24] Denegación de servicio	[0]			
[R-002] REDES ALAMBRICAS	[6]			[8]
[E.2] Errores del administrador	[6]			[8]
[E.25] Pérdida de equipos	[6]			
[A.11] Acceso no autorizado				
[A.24] Denegación de servicio				
[R-003] CONEXION A INTERNET				
[E.2] Errores del administrador				
[E.25] Pérdida de equipos				
[A.11] Acceso no autorizado				
[A.24] Denegación de servicio				

Figura 6.15 Indica el impacto que tendría que una amenaza se materialice en un activo informático

Análisis de los Resultados

En base al Estudio de Análisis de Riesgos realizado en Industrias Catedral podemos evidenciar los activos más importantes

Figura 6.16 Cuadro estadístico de los activos informáticos

Siendo los activos más importantes:

- Sistema Informático General
- Bases de Datos
- Archivos de Trabajo
- Servidores
- Redes Alambricas
- Soportes de Información
- Conexión a Internet

Impacto de las amenazas en los activos informáticos en una escala de 0-10

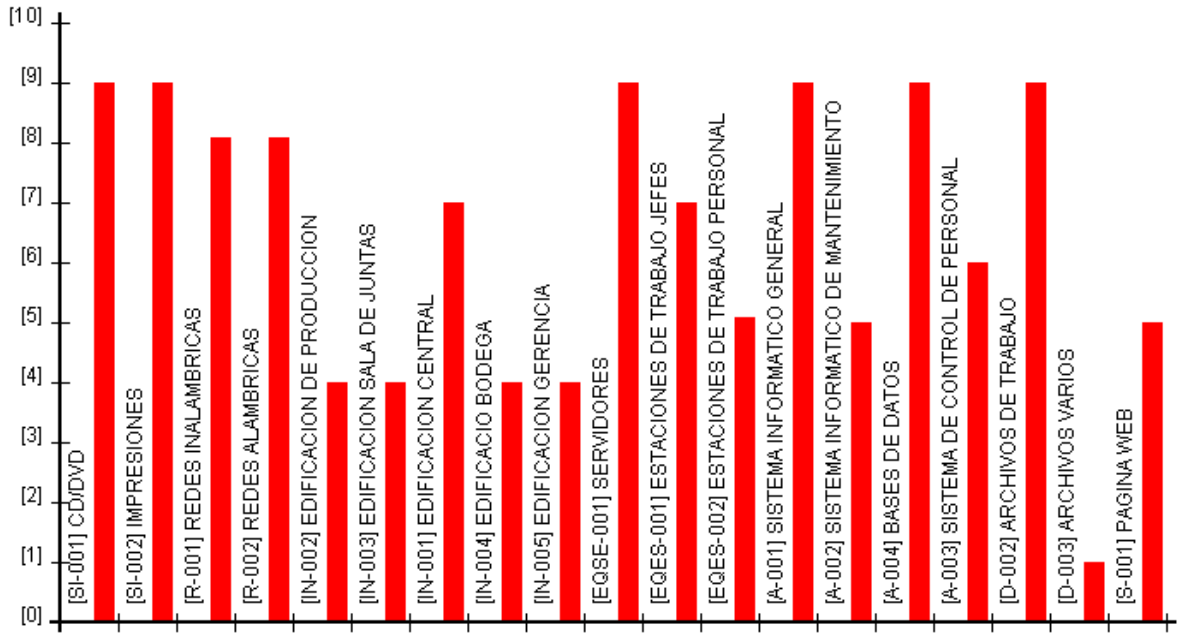


Figura 6.17

El cuadro estadístico indica el impacto que los activos informáticos, al ser vulnerados, tendrían en la organización.

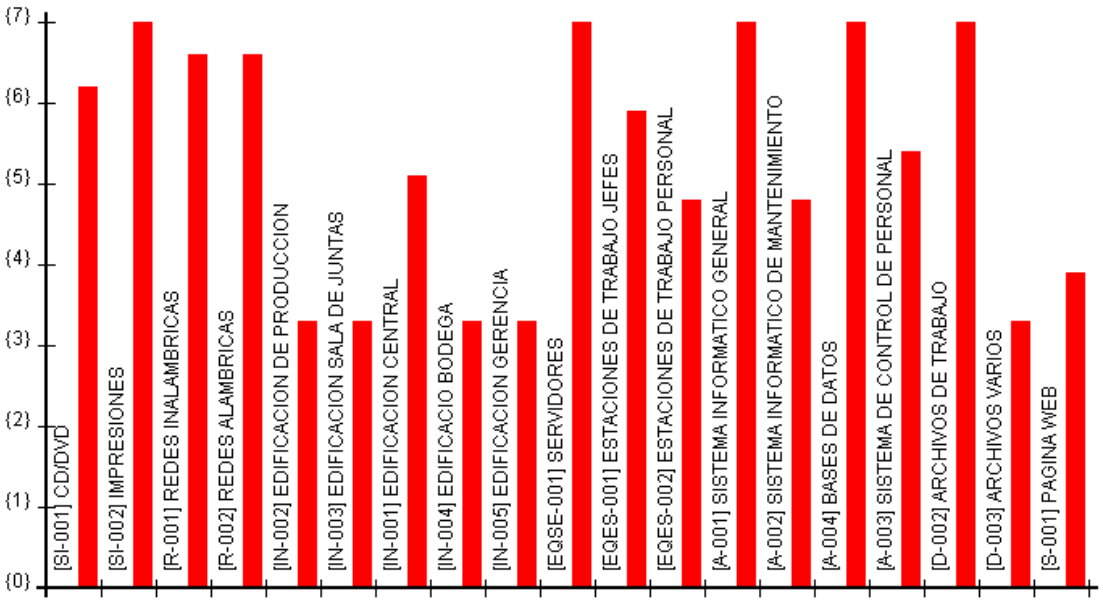


Figura 6.18 **El riesgo que tendría al materializarse una amenaza en los activos informáticos**

Se evidencia que existe un alto porcentaje de amenazas que podrían afectar a los activos informáticos de la empresa. Siendo los más afectadas los siguientes activos

- Sistema Informático General
- Bases de Datos
- Archivos de Trabajo
- Servidores
- Redes Alambricas
- Soportes de Información
- Conexión a Internet

Al ser materializadas estas amenazas podrían alterar el correcto funcionamiento de la organización. Las áreas en las cuales se debe enfatizar son:

Seguridad física y del entorno – Contempla protecciones a los servidores

Seguridad Lógica – Sistema Informático General, Bases de Datos, Archivos de trabajo
Control de accesos – Redes inalámbricas – Conexión a internet

Para disminuir los riesgos informáticos se establecerá Políticas de Seguridad basadas en la norma

Norma ISO/IEC 17799

La Norma ISO/IEC 17799 establece dominios de control que cubren la Gestión de la Seguridad de la Información:

1. Políticas de Seguridad
2. Seguridad ligada al personal: Se orienta a proteger de las acciones del personal que opera con los activos de información. Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.
3. Seguridad física y del entorno: Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.
4. Gestión de comunicaciones y operaciones: Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
5. Control de accesos: Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

6. Cumplimiento o conformidad de la legislación: La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

POLITICAS DE SEGURIDAD INFORMATICA DE INDUSTRIAS CATEDRAL S.A

El Departamento de Sistemas de Industrias Catedral S.A. se encarga de normar el adecuado uso y aprovechamiento de los recursos informáticos, la optimización de actividades, protección de los activos informáticos, proporcionar información veraz, mediante el desarrollo, implantación y supervisión del correcto funcionamiento de los sistemas y comunicaciones, así como la adquisición y control de la plataforma física de computo

Capitulo 1 - Organización Interna

1.1 Generales

a. El Comité de Seguridad Informática de Industrias Catedral deberá estar conformado por la Gerencia General, los responsables de cada proceso y los integrantes del Departamento de Sistemas
b. El personal de Industrias Catedral deberá regirse a los códigos de ética profesional, normas y procedimientos establecidos en la organización
c. Todas las actividades de seguridad de los activos informáticos se llevaran a cabo, basados en la política Industrias Catedral
d. Se nombrara un responsable de la Seguridad Informática, el mismo que tendrá la obligación de cumplir y hacer cumplir las políticas de seguridad informática

1.2 Documentación de Seguridades Informáticas

a. Documentación basada en Análisis de Riesgos
b. Los documentos de Seguridad estarán a cargo del responsable de la Seguridad
c. Se realizara actualizaciones periódicas a los documentos de seguridad

1.3 Sanciones.

a. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento interno de Industrias Catedral S.A.

b. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.
c. Corresponderá al Comité de Informática hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la organización

Capitulo 2 - Protecciones Generales

2.1 Identificación y Autenticación

a. El Responsable de la Seguridad Informática en conjunto con el Jefe de Recursos Humanos serán los encargados de:
   Crea nuevas cuentas de usuario
   Dar de baja cuentas de usuario
b. Para la creación de nuevos usuarios en el Sistema Informático, el Jefe de Recursos Humanos emitirá un **Registro de Ingreso de Personal** al responsable de la seguridad informática, de igual manera para la salida de personal emitirá un **Registro de Salida de Personal**
c. Para la creación de nuevos usuarios y contraseñas se basara en el **Procedimiento de Creación de Nuevos Usuarios**
d. Los usuarios deben:
   Guardar confidencialidad en las contraseñas
   Las contraseñas no se deberán compartir

2.2 Mecanismos de Autentificación

a. El nombre de usuario y contraseña deben ser únicos
b. La contraseña deberá tener una longitud mínima de 6 caracteres – 8 para administradores y 10 para funciones criticas
c. Deberán contener números, letras mayúsculas y minúsculas y caracteres especiales

2.3 Control de Acceso Lógico

2.3.1 Acceso a los Recursos

a. El responsable de la seguridad informática es el ente encargado de proporcionar a los usuarios el acceso a los recursos informáticos, basándose en la **Normativa de Acceso a los Recursos Informáticos.**

b. A nivel general, los permisos de acceso a los recursos informáticos deben estar basados en la necesidad del usuario por conocer la información. Esto implica que los permisos deben ser respaldados y justificados de acuerdo a la función que desempeña el usuario.

c. En casos de emergencia en que los recursos suelen estar desprotegidos y, en las que se requiere que otra persona diferente a la autorizada efectúe un acceso lógico, deberá hacerlo siempre bajo adecuada supervisión. Posterior a la emergencia deberá darse de baja ese usuario y clave o reemplazada con una nueva clave por seguridad.

2.3.2 Control de los Recursos

a. Dado el carácter unipersonal del acceso a la Red, el departamento de Sistemas verificará el uso responsable de la misma.
b. Los sistemas de control de acceso lógico deben contemplar las violaciones al mismo.

2.3.3 Configuraciones Esenciales

a. Uso de una contraseña de inicio para la BIOS
b. Bloqueo de Sesiones de usuario tras dos minutos de inactividad

2.3.4 Gestión de Incidencias

a. Registro de las incidencias de seguridad
b. Registro y control de fallo en el software

Capitulo 3 - Protecciones a la Información

Registro y Control de la Información

a. El Departamento de Sistemas debe llevar un **Inventario de Activos de Información** para el control del mismos
b. El Comité de Seguridad Informática determinara la clasificación de la información, basada en la importancia que esta tenga en la empresa
c. El responsable de la Seguridad Informática deberá establecer mecanismos para asegurar la disponibilidad, la integridad y la confidencialidad de la información
d. Adicional a los mecanismos que utilice deberá existir copias de seguridad de la información critica de cada departamento
e. Se deberá mantener documentado el **Procedimiento de copias de seguridad** y de restauración de las copias de seguridad
f. Las copias de seguridad se mantendrán en un lugar seguro y estará a cargo del Departamento de Sistemas

Capitulo 4 - Protección al Software/Aplicaciones

4.1 De la adquisición de software.

a. Del presupuesto que se designa para el Departamento de Sistemas se utilizara para la adquisición de programación con licencia
b. El departamento de Sistemas deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia o en base a las necesidades de los usuarios.
c. En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor
d. El departamento de Sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguro

4.2 Requisición de Desarrollo de Nuevo Software o cambios

a. Todas las requisiciones de desarrollo de software por parte de los usuarios informáticos se centralizaran en el departamento de sistemas
b. Se deberá especificar los requisitos de seguridad necesarios para la nueva aplicación o actualización de software
c. Se dará seguimiento a las requisiciones
d. En el caso de cambios en el software se basara en el Procedimiento de control de cambios

4.3 De la instalación de software.

a. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).
b. En el caso de que el usuario necesite la instalación de algún software adicional, hará llegar la requisición al Departamento de Sistemas, en ningún caso podrá hacerlo por cuenta propia

4.4 De la actualización del software.

a. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la calendarización que anualmente sea propuesta por el Departamento de Sistemas
b. Corresponde a la Gerencia General autorizar cualquier adquisición y actualización del software.

4.5 De la auditoría de software instalado.

a. El Departamento de Sistemas designara a personal del área para que realicen revisiones periódicas del software que se encuentre instalado en cada equipo esto con el objetivo de garantizar que los recursos informáticos sean utilizados de forma correcta por parte de los usuarios
b. El personal encargado de la revisión emitirá un informe de los hallazgos encontrados

4.6 Del software propiedad de la institución.

a. Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de Industrias Catedral y mantendrá los derechos que la ley de propiedad intelectual le confiera.
b. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de Industrias Catedral S.A. se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.
c. Es obligación de todos los usuarios que manejen información masiva, comunicar al responsable de la seguridad informática, para que esta información sea debidamente respaldada ya que se considera como un activo de la institución que debe preservarse.
d. Los respaldos de los datos, bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.
e. Corresponderá al Responsable de la Seguridad Informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos
f. El Departamento de Sistemas, administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.
g. Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la organización

4.5 Inventario de Software/Aplicaciones

Se mantendrá un registro de aplicaciones de:

- Sistemas Operativo que se utilizan en Industrias Catedral
- Software desarrollado en la empresa y adquirido

4.6 Respaldos de Software/Aplicaciones

a. Se deberá realizar copias de seguridad del software basadas en el **Procedimiento de Copias de Seguridad Informática**

b. La restauración de las copias de seguridad estarán basadas en el Instructivo de restauración de las copias de seguridad

c. Se realizará pruebas de restauración de las copias de seguridad en periodos mensuales

d. Las copias de seguridad se mantendrán en un lugar seguro

Capitulo5 - Protección de los Equipos Informáticos

5.1 Protecciones Generales

a. El uso de los equipos estará regido en base la **Normativa de uso correcto de los equipos**

b. Se deberá realizar un **Inventario de Equipos Informáticos** con sus debidas especificaciones

c. Este inventario deberá ser revisado periódicamente cada 2 meses

d. El departamento de Sistemas deberá garantizar la disponibilidad en todo momento de los equipos informáticos, aplicando alternativas como:

- Adquisición de repuestos
- Mantenimiento preventivo y correctivo solo por personal autorizado
- Equipo alterno

e. Se mantendrá

- registros del mantenimiento preventivo y correctivo
- Procedimiento de copias de seguridad de la configuración
- Procedimiento de restauración de las copias de seguridad

5.2 Protección Física

5.2.1 De la instalación de un equipo de cómputo.

a. Todo equipo de cómputo (computadoras, estaciones de trabajo, impresoras o accesorios de cómputo), que esté o sea conectado a la Red de Industrias Catedral, debe sujetarse al normativa de uso de los mismos
b. Los responsables de los diferentes departamentos deberán en conjunción con el departamento de Sistemas, dar cabal cumplimiento a las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.
c. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, al personal responsable de la seguridad informática

5.2.2 De la actualización del equipo.

Todo equipo de cómputo debe ser actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

5.2.3 De la reubicación del equipo de cómputo.

a. La reubicación del equipo de cómputo se realizará satisfaciendo los procedimientos que el departamento de Informático emita para ello.
b. Se debe notificar los cambios del equipo inventariado (cambio de monitores, de impresoras etc.).

5.3 Adquisición de hardware

Todas las requisiciones de hardware por parte de los usuarios informáticos se centralizaran en el departamento de sistemas

5.4 Perfiles de Seguridad

a. Reducción de los dispositivos a los mínimos necesarios
b. Configuración segura de los dispositivos activados

c. Retirada de componentes innecesarios

5.5 Seguridad de los equipos fuera de las instalaciones

Deberá existir un Registro de salida del equipo, el mismo que estará autorizado por la Gerencia General

5.6 Cambios

a. Definición del proceso de cambio de tal forma que minimice la interrupción
b. Se realizara por personal debidamente autorizado
c. Se llevara un registro de todo cambio que se realice en el hardware

5.7 Terminación

Un equipo informático se dará de baja en base al Procedimiento de baja de Equipos informáticos establecido por el Departamento de Sistemas

Capitulo 6 - Protección de las Comunicaciones

6.1 De utilización de los recursos de la red

a. Los recursos disponibles a través de la Red serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de Industrias Catedral
b. El Departamento de Informática es el ente responsable de emitir y dar seguimiento a la Normativa para el uso de la Red.
c. Corresponde al Departamento de Sistemas administrar, mantener y actualizar la infraestructura de la Red

6.2 Se debe asegurar la disponibilidad de las comunicaciones para ello se deberá

d. Identificar y eliminar los puntos únicos de fallo
e. Adquisición de repuestos
f. Monitoreo de enlaces y dispositivos de red

g. Conexión redundante de la red

6.3 Se mantendrá perfiles de seguridad a través de:

Eliminación de cuentas estándar de usuario con las que vienen por defecto los dispositivos

6.4 Acceso al Internet

a. El uso de Internet dentro de la organización está regido por la Normativa de uso o acceso a Internet
b. Se controla el consumo de ancho de banda por parte de los usuarios
c. Se mantendrá un Registro de navegación web de cada usuario

6.5 Disponibilidad de la wireless

a. La Red Wireless estará disponible para aquellos usuarios informáticos que consten en la normativa de Autorización de puntos de acceso
b. Se utilizara algún mecanismo para el Control de direcciones IP que se encuentren conectadas a la red
c. Comprobación Periódica de los puntos de acceso

Capitulo 7 Protección de los Soportes de Información

7.1 Generales

a. Se mantendrá un inventario de los soportes de información clasificado en críticos y normales
b. Según la vida útil de los soportes de información se deberá migrar los datos
c. El almacenamiento de los soportes críticos será en un lugar seguro

7.2 Gestión de Soportes

a. Revisiones periódicos de las listas de distribución y destinatarios
b. Restricciones de acceso para impedir el acceso no autorizado

7.3 Etiquetado

a. Procedimiento para el etiquetado y marcado en dependencia de su contenido
b. Etiquetado de todos los soportes de datos indicando su nivel de clasificación

7.4 Destrucción de soportes de información

- **a.** Se mantendrá un Registro de destrucción del soporte de información que se ha dado de baja
- **b.** Control de acceso a los soportes de información que van a ser eliminados

Capitulo 8. Protección de las instalaciones

8.1 Diseño y Ubicación

Se deberá separar las áreas de seguridad y de acceso público

8.2 Control de accesos

a. Solo personal autorizado podrá acceder a las instalaciones
b. Accesos cerrados fuera de las horas de trabajo

Capitulo 9 - Gestión del personal

9.1 Se deberá mantener Acuerdos de confidencialidad entre Industrias Catedral y los usuarios informáticos

Se identificara los requisitos de seguridad de la información de cada uno de los puestos

1. Asignación de la responsabilidad de seguridad de los puestos
2. En el caso que el personal sea reubicado en otro puesto de trabajo se actualizaran los acuerdos de confidencialidad
3. **Contratación**
   - **d.** Términos y condiciones de la relación laboral
   - **e.** Inclusión del ámbito, el alcance y las responsabilidades de seguridad de los activos informáticos
   - **f.** Inclusión de acuerdos de confidencialidad en los contratos laborales
   - **g.** Finalización de la relación laboral

9.2 Plan de formación y concienciación

Procedimientos y Normativas relevantes de seguridad

- **Procedimiento de Creación de Usuarios**

Para la creación de usuarios y sus contraseñas se basara en:

1. Es función del encargado del proceso de Recursos Humanos emitir el registro de ingreso de personal

INDUSTRIAS CATEDRAL S.A. **INGRESO DE PERSONAL** **Nombre del Empleado:** …….. **Fecha de Ingreso:**…… **Función que va a desempeñar**
Área para el responsable de la Seguridad
……. ……. **Jefe de Recursos Humanos** **Responsable de la Seguridad**

2. Identificación de los usuarios

- En base a la función que va a desempeñar, el responsable de la seguridad llenara el campo del registro designado para él, con el nombre de usuario y contraseña, accesos a la información según corresponda
- Para cada usuario se definirá:

nombre de usuario y contraseña para ingreso al Sistema Operativo

nombre de usuario y contraseña para ingreso al internet en el caso de que sus funciones así lo requiera

nombre de usuario y contraseña para los Sistemas Informáticos en caso de requerirlo

PROCEDIMIENTOS PARA ACCESO A LOS RECURSOS INFORMÁTICOS

A nivel general, los permisos de acceso a los recursos informáticos deben estar basados en la necesidad del usuario por conocer la información. Esto implica que los permisos deben ser respaldados y justificados de acuerdo a la función que desempeña el usuario.

Función: Jefe Financiero		
Sistema Informático	**Servicios**	**Software**
Contabilidad	Internet	Microsoft Office
Costos	Chat Interno	
Presupuestos		

Función: Asistente de Contabilidad - Pagos		
Sistema Informático	**Servicios**	**Software**
Caja	Internet	Microsoft Office
Caja Chica	Chat Interno	
Bancos		
Viáticos		

Función: Asistente de Contabilidad – Compras		
Sistema Informático	**Servicios**	**Software**
Caja	Internet	Microsoft Office
Bancos	Chat Interno	Adobe Ilustrator
Compras		Corel Draw
Anexos Transaccionales		
Sistema del SRI		

Función: Asistente de Contabilidad		
Sistema Informático	**Servicios**	**Software**
Caja		Microsoft Office
Caja Chica	Chat Interno	REOC
Bancos		
Viáticos		

Función: Jefe de Recursos Humanos		
Sistema Informático	**Servicios**	**Software**
Roles de Pago	Internet	Microsoft Office
Control de Horas	Chat Interno	

Función: Asistente de Recursos Humanos		
Sistema Informático	**Servicios**	**Software**
Roles de Pago	Internet	Microsoft Office
Control de Horas	Chat Interno	Sistema del Produbanco

Función: Jefe de Ventas		
Sistema Informático	**Servicios**	**Software**
Reportes	Internet	Microsoft Office
	Chat Interno	

Función: Asistente de Ventas 1		
Sistema Informático	**Servicios**	**Software**
Reportes		Microsoft Office
Pedidos	Chat Interno	
Facturación		

Función: Asistente de Ventas 2		
Sistema Informático	**Servicios**	**Software**
Ninguno	Chat Interno	Microsoft Office

Función: Facturación		
Sistema Informático	**Servicios**	**Software**
Facturación		Microsoft Office
Viáticos	Chat Interno	

Función: Secretaria		
Sistema Informático	**Servicios**	**Software**
Ninguno	Internet	Microsoft Office
	Chat Interno	

Función: Asistente de Producción		
Sistema Informático	**Servicios**	**Software**
Producción	Chat Interno	Microsoft Office

Función: Jefe de Producción		
Sistema Informático	**Servicios**	**Software**
Producción	Internet	Microsoft Office
	Chat Interno	

Función: Jefe de Mantenimiento		
Sistema Informático	**Servicios**	**Software**
Mantenimiento	Internet	Microsoft Office
	Chat Interno	Auto Cad

Función: Supervisor de Control de Calidad		
Sistema Informático	**Servicios**	**Software**
Producción	Chat Interno	Microsoft Office

Función: Asistente de BPM		
Sistema Informático	**Servicios**	**Software**
Ninguno	Chat Interno	Microsoft Office

Función: Jefe de Bodega		
Sistema Informático	**Servicios**	**Software**
Inventarios	Chat Interno	Microsoft Office

Función: Asistente de Bodega		
Sistema Informático	**Servicios**	**Software**
Inventarios	Chat Interno	Microsoft Office

Procedimiento de Copias de Seguridad de la Información Crítica de Industrias Catedral

1	Se realizarán automáticamente backups diarios de las carpetas que contengan la información critica de cada departamento, para lo cual se debe considerar la configuración del software Cobian Backup que contiene programadas las carpetas a respaldar y cuyo respaldo se ejecutará a las 18h00 de todos los dias laborables, en el disco duro externo conectado como unidad de red X del servidor central, el nombre de la carpeta será informacioncritica mas la fecha del día que corresponda	Jefe de Sistemas	Medio Magnético externo Debidamente etiquetado
2	Para las bases de datos SQL Server 2000, los backups se generarán conforme los trabajos programados en el Agente SQL Server, los mismos están etiquetados como findeldia(nombre de la base de datos), estos respaldos se almacenan en el disco duro externo X en la carpeta SQL del servidor central y se etiquetarán de la siguiente manera Nombredelabasededatos+año+mes+dia.bak	Jefe de Sistemas	Medio Magnético externo Debidamente etiquetado
3	Las aplicaciones se respaldaran una vez al dia y se lo hará automáticamente según el software Cobian Backup	Jefe de Sistemas	Medio Magnético externo Debidamente etiquetado

Copias de Seguridad fuera de las instalaciones de la empresa

1	Se creará una carpeta llamada Información Total esta contendrá respaldos de la Información critica, bases de datos y aplicación de la empresa	Jefe de Sistemas	
3	Dicho disco será entregado al Gerente General quién firmará un documento de entrega del dispositivo.	Jefe de Sistemas	Documento De Entrega
4	Gerente General se encargará de llevar el dispositivo a la entidad donde se encuentra el casillero de seguridad de la empresa	Gerente General	
5	Esta información de ser el caso deberá ser cargada en el motor de las bases de datos del servidor alterno para su posible utilización en el caso de una catástrofe informática de la organización. De igual forma las aplicaciones Y la Información Critica	Jefe de Sistemas	

Normativa de Uso de los Equipos Informáticos

Entiéndase como Equipo -Computacional todas las computadoras personales, scanners, proyectores, plotters e impresoras. Para el uso se considerará:

a) El equipo de computo debe ser utilizado en labores inherentes a las funciones encomendadas,
b) El cuidado y limpieza de los equipos computacionales son responsabilidad exclusiva del custodio del bien,
c) Los equipos deberán permanecer encendidos solamente en horas laborables, para evitar el consumo innecesario de energía.

d) Los usuarios que detecten daños o anomalías en el equipo computacional deberán reportarlos de forma inmediata al Departamento de Sistemas

e) Todo lo que devenga del mal uso del equipo será de responsabilidad del custodio.

f) Las unidades para la recarga de impresión (tóners, cintas y cartuchos de tinta) serán entregadas al usuario que las solicite previa presentación de la unidad recién acabada.

g) El Departamento de Sistemas llevará un control bimensual de la periodicidad de la recarga de las impresoras, con el fin de establecer el rendimiento de las unidades de recarga.

h) Los usuarios se comprometerán a optimizar el uso de los recursos de impresión.

i) Está prohibido manipular comidas, bebidas o fumar cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterioro del mismo, en estos casos se informará vía documento a la Jefatura correspondiente

INVENTARIO DE EQUIPOS INFORMATICOS

SERVIDORES

N º	EQUIPO	PROCESADOR	MEMORIA	CAPACIDAD DE DISCO DURO	AÑO DE COMPRA
1	SE-001 Servidor Central	INTEL XEON	2 GIGAS	146	2009
2	SE- 002 Servidor Backup	INTEL XEON	2 GIGAS	146	2007
3	SE-003 Servidor Proxy	INTEL CORE 2 DUO DE 1.8 GHZ	2 GIGAS	250	2007

ESTACIONES DE TRABAJO

Nº	EQUIPO	PROCESADOR	MEMORIA	DISCO DURO	AÑO
1	ES-001 Equipo de Secretaria	INTEL CORE 2 DUO	2 GIGAS	250	2010
2	ES-001 Equipo de Contabilidad (Contadora)	INTEL CORE 2 DUO	3 GIGAS	200	2008
3	ES-002 Equipo de Auxiliar Contable	INTEL PENTIUM 4	512 MEGAS	250	2006
4	ES-001 Equipo de Auxiliar de Contabilidad (Compras)	MACBOOK PRO	4 GIGAS	150	2010
5	ES-001 Equipo de Auxiliar de Contabilidad (Pagos)	INTEL CORE 2 DUO	1 GIGA	250	2008
6	ES-001 Equipo de Caja	INTEL PENTIUM 4 DE 2.8 GHZ	1 GIGA	130	2004
7	ES-001 Equipo de Ventas (Jefe de Ventas)	INTEL CORE 2 QUAD	2.4 GIGAS	500	2008
8	ES-002 Equipo de Auxiliar de Ventas1	INTEL CORE 2 QUAD	2.4 GIGAS	500	2008
9	ES-002 Equipo de Auxiliar de Ventas2	INTEL PENTIUM 4 DE 1.4 GHZ	128 MB	20	2001
10	ES-001 Equipo del Punto de Ventas	INTEL QUAD CORE	1 GIGA	250	2010
11	ES-002 Equipo de Facturación	INTEL CORE 2 DUO DE 1.8 GHZ	512 MB	150	2007
12	ES-002 Equipo de Producción	INTEL QUAD CORE DE 2.4GHZ	1 GIGA	300	2007
13	ES-002 Equipo de Auxiliar de Producción	INTEL PENTIUM 4	512 MB	250	2006
14	ES-002 Equipo de Bodega (Jefe de Bodega)	INTEL PENTIUM 4 DE 2.8 GHZ	1 GIGA	120	2005
15	ES-002 Equipo de Bodega (Asistente de Bodega)	INTEL CORE 2 DUO	2 GIGAS	230	2007
16	ES-001 Equipo de Sistemas (Jefe de Sistemas)	INTEL CORE 2 DUO	1 GIGA	250	2007
17	ES-001 Equipo de Recursos Humanos (Jefe de RR HH)	INTEL CORE 2 DUO DE 2.8 GHZ	2 GIGAS	250	2009
18	ES-002 Equipo de Asistente de Recursos Humanos	INTEL CORE 2 DUO DE 2.8 GHZ	3 GIGAS	250	2009
19	ES-002 Equipo de Control de Calidad	INTEL PENTIUM 4 DE 2.8 GHZ	1 GIGA	130	2004
20	ES-001 Equipo de BPM	INTEL PENTIUM 4	512 MB	80	2005
21	ES-001 Equipo de Mantenimiento	INTEL CORE 2 DUO DE 2.19 GHZ	1 GIGA	150	2008

Normativa del lugar de ubicación del equipo Informático

- El equipo de la empresa que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de:

  Seguridad física

  - Ubicación adecuada de los equipos (evitar accesos innecesarios, daños por agua)
  - Los elementos que requieran especial protección se aislaran para aumentar el nivel de protección requerido

- Las condiciones ambientales
- La alimentación eléctrica

Normativa del Uso de la Red

El uso de los servicios de la red será exclusivamente con fines laborales, lo que excluye cualquier uso comercial de la red o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la misma, tanto en las prestaciones de ésta como en la privacidad de su información.

Derechos del usuario

a) Utilizar los servicios de la red de datos de la empresa para llevar a cabo las labores inherentes a sus funciones
b) Compartir e intercambiar archivos mediante "carpetas compartidas" entre usuarios que lo necesitasen para el desempeño de sus actividades laborales.

Restricciones para el uso de la Red de Datos.- En particular quedan expresamente restringidas las siguientes acciones:

a) Usar indebidamente los sistemas o equipos conectados a la Unidad y otras redes a las que se proporcione acceso; si por esta razón se ocasionan daños, el usuario será responsable de los mismos.

b) Ingresar en otros Computadores Personales que formen parte de la red, sin la autorización correspondiente.

c) Diseminar virus y otros tipos de programas dañinos en la red

d) Utilizar los medios de la red con fines propagandistas o comerciales.

e) Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso propio del trabajo.

f) Acceder, analizar, modificar o exportar archivos a los cuales no se tengan la autorización respectiva.

g) Interferir o interrumpir redes conectadas con el servicio o infringir las normas, directivas o procedimientos de dichas redes.

Normativa del uso de Internet

Asignación del Servicio de Internet.- El Departamento de Sistemas, ofrece el servicio de Internet a todo el personal que lo necesite.

Cuidados con el contenido.- Evitar descargar archivos de origen no autorizado, y acceder a páginas no autorizadas, por el riesgo de contraer virus y código malicioso que afectan el rendimiento de los equipos de informática.

Sobre el acceso a internet y otros servicios web

No está permitido el uso indebido de los recursos de internet con fines personales

No está permitido acceder a internet con fines comerciales o recreativos (juegos, chat, radio por internet, blogs de música y video para descargar o escuchar en línea, conversación en tiempo real).

No está permitido degradar el ancho de banda de la conexión de Internet, debido a descargas de archivos de música, imágenes, videos, etc., o empleo de radio o video en línea, no autorizado.

Notas

1. Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.
2. El documento que contiene la política de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas.

Glosario.

Departamento de Sistemas

Es la entidad encargada de ofrecer sistemas de información administrativos permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias de cada uno de los departamentos de Industrias Catedral

Responsable de la Seguridad

Es la persona encargada de controlar buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución. Así como también implementar las seguridades informáticas necesarias para proteger los activos informáticos de Industrias Catedral

Bases de Datos.

Es una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápida.

WWW (World Wide Web).

Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de internet en una forma fácilmente accesible. Sistema avanzado para navegar a través de internet.

Equipo de Telecomunicaciones.

Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Equipo de Cómputo.

Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

IP - Internet Protocol.

Parte de la familia de protocolos TCP/IP, que describe el software que supervisa las direcciones de nodo internet, encamina mensajes salientes y reconoce los mensajes entrantes.

Control de Acceso.

Una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones

PLAN DE ACCION

Descripción	Abril	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre
Revisión y Aprobación por la Gerencia General									
Capacitación al Personal de Sistemas sobre el proceso a seguir									
Difusión de las Políticas de Seguridad Informática en la empresa									
Implantación de las Políticas de Seguridad Informática									
Revisión de las Políticas de Seguridad Informática									

Administrativo

Personal Administrativo	
Cargo	**Nombre**
Presidente	Sra. Carmen Buenaño
Gerencia General	Ing. Javier Buenaño
Jefe Financiero	Dra. Patricia Benalcázar
Asistente Contabilidad	Dra. Verónica León
Asistente Contabilidad	Ing. Darwin Masaquiza
Asistente Contabilidad	Dra. Isabel Dávalos
Asistente Contabilidad	Dra. Silvia Bonilla
Secretaria	Abg. Mónica Cevallos
Personal de Producción	
Jefe de Producción	Ing. Jorge López
Asistente de Producción	Lcdo. Jorge Mancero
Personal de Recursos Humanos	
Jefe de Recursos Humanos	Dr. Hendry Yagchirema
Personal de Ventas	
Jefe de Ventas	Sr. Victor Hugo Buenaño
Asistente de Ventas	Srta. Gabriela Almeida
Asistente de Ventas	Lcdo. Omar Guamarica
Asistente de Ventas	Ing. Olger Jaramillo
Personal de Bodega de Producto Terminado	
Jefe de Bodega	Ec. Jaime Buenaño
Asistente de Bodega	Sr. Rodolfo Pillajo
Personal de Mantenimiento	
Jefe de Mantenimiento	Ing. Gabriel Naranjo
Personal de Control de Calidad	
Supervisor de Calidad	Ing. Medardo Garcés
Asistente de BPM	Ing. Paola Cando
Asistente de BPM	Ing. Carmen Arroba

Previsión de la Evaluación

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Quiénes solicitan proteger los activos informáticos?	Gerencia General de Industrias Catedral S.A.
¿Por qué proteger?	Porque el aumento de ataques informáticos ha aumentado significativamente, ocasionando incertidumbre a los altos mandos.
¿Para qué proteger?	Para garantizar la disponibilidad, confidencialidad, integridad y la autenticidad en todos los activos informáticos de la empresa
¿Qué proteger?	Los diferentes activos informáticos.
¿Quién será el encargado de establecer medias de protección?	El responsable de la Seguridad Informática.
¿Cuándo proteger?	Inmediatamente luego de la revisión y aprobación gerencial
¿Cómo proteger?	Utilizando Políticas de Seguridad Informática.
¿Con qué proteger?	Con las Políticas de Seguridad Informática

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El Análisis de Riesgos, ha permitido determinar los activos de mayor importancia, el impacto que tendría el que una amenaza se materialice y el riesgo que existe

En base a los datos que ha dado el análisis de riesgos se ha establecido los salvaguardas necesarios para proteger los activos de mayor importancia y minimizar el riesgo de que las amenazas se materialicen

Las Políticas de Seguridad Informática propuestas en el presente proyecto brindaran un alto porcentaje de seguridad a los activos informáticos

Recomendaciones

Controlar el cumplimiento de las políticas planteadas en un alto porcentaje

Dar un seguimiento a los salvaguardas planteados en el presente proyecto para estimar el riesgo residual en los activos informáticos de Industrias Catedral S.A.

BIBLIOGRAFÍA

HATCH,Brian
LEE, James
KURTZ, George
Hackers en Linux , Mc Graw-Hill,2001

MARTINEZ, José Andrés
Linux la referencia Visual ,Editorial Mc Graw-Hill , Primera Edición, Colombia, 2001.

PETERSEN, Richard
Linux manual de referencia, Mc Graw-Hil, Segunda Edición, España, 2001.

DIRECCIONES DE INTERNET

http://ataquesinformaticos.blogspot.com/ - Ataques Informaticos

http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares esquemas/ISOIEC-27001 - Normas ISO

http://www.delitosinformaticos.com/seguridad/clasificacion.shtml - Delitos Informáticos

http://www.inforsist.net/articulo.php?id=35 – Seguridad Informática

http://www.inforsist.net/articulos.php?sec=unix – Seguridad Informática

http://educativa.catedu.es/22700133/aula/archivos/repositorio//0/31/Instrucciones_envio recepcionbaja_equipos.pdf - Intrusiones a los Sistemas Informáticos

http://intranet.dgcft.sep.gob.mx/uploads/CRITERIOS%20TEC%20PARA%20BAJA%20BIENES%20INF.pdf

http://jcerpa.blogspot.com/2010/05/lopd-registro-de-incidencias.html

http://www.medicina.usmp.edu.pe/comites/acreditacion/documentacion/11_infraestructura/pdf/REGLAMENTO%20DE%20LA%20UNIDAD%20DE%20COMPUTO_comp.pdf

http://www.uc3m.es/portal/page/portal/orientacion_personal_participacion/asociaciones/recursos_servicios/normas_uso_equipos_informaticos

http://www.upch.edu.pe/dui/userdocs/doku.php?id=usuarios:procedimientos:registro_y_baja_de_un_usuario

http://es.wikipedia.org/wiki/Magerit

http://www.coit.es/publicac/publbit/bit128/bitcd1/legisla/pg5m21.htm
http://www.gigle.net/espana-incluye-nuevos-delitos-informaticos-en-el-codigo-penal/
http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=99%3A-reglamento-a-la-ley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos&Itemid=103

ANEXOS

Encuesta realizada al personal Administrativo de Industrias Catedral

Nº	Preguntas	Respuestas
1	¿Se le ha capacitado sobre las medidas de seguridad informática existentes en la empresa?	SI NO
2	¿Está instalado en su equipo algún programa de protección de la información?	SI NO
3	¿Cada qué tiempo se actualiza el antivirus en su máquina?	Semanal Mensual Automáticamente
4	¿En algún momento, la información que Ud. maneja fue:	Alterada Borrada Ninguna
5	Se le ha mencionado sobre los cuidados que debe darle al equipo de computo que está a su cargo?	SI NO
6	¿En alguna ocasión su equipo se ha dañado y ha perdido información relevante de su proceso?	SI NO
7	¿Ha instalado programas aplicaciones a los previamente instalados en su equipo?	SI NO
8	¿Ud. puede acceder a la información que se encuentre en los equipos de la red o unidades compartidas?	SI NO
9	¿Desde el momento que le asignaron	SI

	un equipo de cómputo, fue creado su usuario de ingreso al equipo?	NO
10	¿Ud. puede acceder a la información que se encuentra en los servidores centrales?	SI NO
11	¿Le hablaron sobre la confidencialidad que debe existir en el manejo de una contraseña y de la responsabilidad que ésta conlleva?	SI NO
12	¿Tiene conocimiento Ud. sobre una incidencia de seguridad de la información en la empresa?	SI NO

Entrevista realizada al Jefe de Sistemas

Objetivo: Determinar las actividades de Seguridad Informática que se realiza

Preguntas	Respuestas
El nivel de Seguridad Informática que existe en Industrias Catedral es:	Alto Medio Bajo
En Industrias Catedral se realizan actividades de Seguridad Informática como:	Escaneo de Puertos Monitorización de la red Auditoria de los Equipos Informáticos Sistemas de Detección de Intrusos Ninguna
Existe actividades ligadas al personal como:	Capacitación al Personal sobre incidencias de Seguridad Acuerdos de Confidencialidad entre La empresa y el empleado Procesos Disciplinarios para quienes violen la seguridad Controles de Acceso a la Información
La información importante de la empresa es respalda en :	La empresa Fuera de la empresa Ninguna Ambos
El área de los equipos informáticos esta implementada con:	Temperatura Adecuada Sistema de Alarma (humo, fuego, etc.)

Preguntas	Respuestas	
Existe en Industrias Catedral un Plan de Mantenimiento	Preventivo	☐
	Correctivo	☐
	Ninguno	☐
Los soportes de Información que ya no se utiliza son:	Dados de Baja	☐
	Reutilizados	☐
	Archivados	☐
	Ninguno	☐
Los activos informáticos están clasificados en base a:	Servicios	☐
	Datos/Información	☐
	Aplicaciones	☐
	Equipos Informáticos	☐
	Redes de Comunicación	☐
	Soportes de Información	☐
	Instalaciones	☐
	No Existe Clasificación	☐
El criterio de Valoración de los activos esta dado en base a:	Disponibilidad	☐
	Integridad	☐
	Confidencialidad	☐

Preguntas	Respuestas
El registro de un Activo Informático contiene datos como:	Ubicación ☐ Responsable ☐ Fecha de Entrega ☐ Características del Equipo ☐ No existe Registro ☐

Industrias Catedral S.A.
Inventario de la Información Critica

Fecha: **Tipo de Clasificación: ……..**

N	Descripción	Responsable	Observación

Elaborado por:
……..

DEPARTAMENTO DE SISTEMAS **RG-SI-01**
SOLICITUD Nº _____

Fecha de Solicitud: _____ Solicitante _____

Proceso: _____

Fecha proyectada de entrega: _____

DESCRIPCION DE LO REQUERIDO

_____	_____	_____
Firma de Petición	Recibí conforme	Autorizado Por

DEPARTAMENTO DE SISTEMAS **RG-SI-04**

REGISTRO DE SEGUIMIENTO DE SOLICITUD

Número de Solicitud Realizada: _____

Proceso: _____

Fecha de Seguimiento: _____

Fecha Máxima de Auditoria: _____

OBSEVACION

Firma de Conformidad

DEPARTAMENTO DE SISTEMAS **RG-SI-02**

REGISTRO DE SOLICITUD CONLCUIDA Y ENTREGADA

Número de Solicitud Realizada: _____

Proceso: _____

Fecha Real de Entrega : _____

OBSERVACIONES

Firma de Conformidad